Co-funded by the European Union

KOBİ SIBER GÜVENLIK DEĞIŞIM AJANLARI EĞITIMI IHTIYAÇ HARITALAMA RAPORU

CYBER AGENT 10.2023

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

İş Paketi 2: CyberAgent yaklaşımı ve yapı tasarımı

Teslim 2.2: KOBİ Siber Güvenlik Değişim Ajanları Eğitimi ihtiyaç haritalama raporu

WP2 Lideri – Olemisen Balanssia ry
Teslim edilebilir 2.2 Lideri – Olemisen Balanssia ry

İÇERİK

GIRIŞ

Bu proje raporu, bir KOBİ Siber Güvenlik Değişim Temsilcisi için gerekli olan uygun yeterlilikleri belirlemek için eğitim ihtiyaçlarını analiz etmeyi ve haritalamayı amaçlamaktadır. Bu rapor, mevcut eğitim tekliflerinin kapsamlı bir incelemesi ve KOBİ'lerin siber güvenlik konularına ilişkin tercihlerini anlayarak, mevcut yetkinlikler arasındaki boşluğu kapatmayı ve gerekli ideal beceri setini tanımlamayı amaçlamaktadır.

Siber tehditlerin karmaşıklığı arttıkça, KOBİ'lerin bu tehditlerle mücadele etmek için yeterli eğitimli personele sahip olduklarından emin olmalarına güçlü bir ihtiyaç vardır. Siber güvenlik alanındaki değişim ajanları bu bağlamda çok önemli bir rol oynamaktadır. Bu proje raporu, siber güvenlik ortamını farklı bakış açılarıyla analiz ediyor: Eğitim ve öğretim, cinsiyet kapsayıcılığı ve KOBİ'lerde ve okul kurumlarında mevcut durum.

1. METODOLOJİ

Bu haritalama işlemi için masa başı ve saha araştırmasını birleştiren karma bir yaklaşım kullandık.

Masa başı araştırmasında kapsamlı bir literatür taraması yapılmıştır:

- Her ortak ülkede siber güvenlik alanında Mesleki Eğitim ve Öğretim seviyelerinde mevcut ve ortaya çıkan eğitim hükümlerini gözden geçirin. Siber güvenlik eğitim içeriği ve ihtiyaçları ile ilgili makaleler, teknik incelemeler, araştırmalar ve raporlar bulmak ve derlemek.
- Mesleki Eğitim ve Öğretim kurslarını, müfredatlarını ve gerçek dünyadaki siber güvenlik zorluklarıyla olan ilgilerini analiz edin.

Hedefler şunlardı:

- Her ülkede Mesleki Eğitim ve Öğretim seviyelerinde sunulan siber güvenlik derslerinin mevcut müfredat bileşenlerini belirlemek.
- Bu müfredatların siber güvenlik zorluklarıyla nasıl uyumlu olduğunu değerlendirmek.
- Siber güvenlik çalışmalarına daha fazla kadını dahil etmek için belirli stratejiler veya programlar olup olmadığını belirleyin.

Saha araştırması aşamasında 2 anket çalışması gerçekleştirdik. Her ülkeden hem Mesleki Eğitim hem de Öğretim kategorilerinden öğretmenler ve eğitmenler için mevcut eğitim hükümlerinin nüanslarını anlamak için tasarlanmıştır. Diğeri, şirketlerde siber güvenlikle ilgili durum hakkında bir görüş ve anlayış elde etmek için KOBİ'lere göre uyarlanmıştır: Çalışanların bu konulara nasıl dahil olduğu ve dahil olduğu, zorluklar ve ihtiyaçlar. Bu saha araştırmasının odak noktası, özellikle siber güvenlikte kadınların ihtiyaçlarını vurgulayarak, özellikleri, eğitim ihtiyaçlarını ve öğrenme tercihlerini belirlemekti.

Her iki anket için de önemli sayıda cevaba ulaştık. Mesleki Eğitim ve Öğretim kurumlarından 190 öğretmen ve eğitmen ve KOBİ çalışanlarından 176.

Anket 1: KOBİ Siber Güvenlik Değişim Ajanları için eğitim ihtiyaçlarının haritalandırılması - **Mesleki Eğitim ve Öğretim ve HEI anketi.**

Kurum türü	**Yanıt**	**Dişi**	**Erkek**	**Söylememeyi tercih ederim**
HEI (Yüksek Öğretim Kurumları)	104	28	73	3
VET (Mesleki Eğitim ve Öğretim)	86	36	48	2
Toplam	**190**	**64**	**121**	**5**

Anket 2: KOBİ Siber Güvenlik Değişim Ajanları - **KOBİ'ler anketi için eğitim ihtiyaçlarının haritalandırılması.**

Yanıt sayısı	**Sayı**
KOBİ'ler	176
Toplam	**176**

Anketler ve tüm veriler Ek C ve D'de bulunabilir.

2. ARAŞTIRMA (TÜM ORTAKLAR)

2.1. MEVCUT EĞITIM VE ÖĞRETIM HÜKÜMLERI

Bu bölüm, ortak ülkelerdeki mevcut eğitim ve öğretim altyapısındaki güçlü yönleri ve boşlukları vurgulayarak araştırmayı sunar ve masa başı araştırma ve anketlerden elde edilen içgörüleri sağlar.

2.1.1. MESLEKI EĞITIM VE ÖĞRETIM SIBER GÜVENLIK EĞITIMINE GENEL BAKIŞ

Mevcut durumunu tanımlamak ve siber güvenlik eğitimi ve öğretiminin ilgili yönlerini tetiklemek için tüm ortak ülkelerdeki siber güvenlik eğitimi ortamının geniş bir analizini gerçekleştirdik.

Litvanya'da,[1] AIKOS veritabanında yapılan bir araştırma, Litvanya kurumları tarafından sunulan ve hem lisans hem de yüksek lisans seviyelerini kapsayan toplam altı resmi siber güvenlik eğitim programını ortaya çıkardı:

Çalışma yönü	Program	Kuruluş	Dersin AKTS Kredisi	Derece
Bilişim mühendisliği	Bilgi ve Bilgi Teknolojileri Güvenliği[2]	Kaunas Teknoloji Üniversitesi	120	Bilgisayar Bilimleri Yüksek Lisansı
Yönetim	Siber Güvenlik Yönetimi[3]	Mykolas Romeris Üniversitesi	90	İşletme Yönetimi Yüksek Lisansı
Bilişim mühendisliği	Bilgi ve bilgi teknolojileri güvenliği[4]	Vilnius Gediminas Teknik Üniversitesi	120	Bilgisayar Bilimleri Yüksek Lisansı
Bilişim mühendisliği	Bilişim Sistemleri ve Siber Güvenlik[5]	Vilnius Üniversitesi	210	Bilgisayar Bilimleri Lisansı
Bilişim mühendisliği	Bilişim Sistemleri ve Siber Güvenlik Teknolojileri[6]	Marijampole Koleji	180	Profesyonel Bilgisayar Bilimleri Lisansı
Bilişim mühendisliği	Siber Sistemler ve Güvenlik[7]	Kaunas Koleji	180	Profesyonel Bilgisayar Bilimleri Lisansı

Yüksek lisans düzeyindeki siber güvenlik programları, farklı ancak tamamlayıcı yaklaşımlar sergiler. Kaunas Üniversitesi, güvenli BT sistem tasarımı ve uygulama becerilerinin

[1] Program aramada kullanılan anahtar kelimeler *siber, güvenlik* ve bunların varyasyonlarıydı. Kaynak: https://www.aikos.smm.lt/Puslapiai/Pradinis.aspx
[2] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=8618_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[3] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2845&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[4] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=1442_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[5] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=9664&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[6] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2775&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[7] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=3797&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d

geliştirilmesine odaklanarak araştırma metodolojisini, bilgi güvenliği yöntemlerini ve elektronik alanın yasal yönlerini vurgulamaktadır. Vilnius Gediminas Teknik Üniversitesi, eleştirel düşünmeyi ve liderliği teşvik etmenin yanı sıra, bilgi güvenliği konularına sistematik bir yaklaşımla uzmanlar oluşturmaya, bilimsel bilgiyi bilgi güvenliğini sağlamaya yönelik yöntem ve teknolojilerle harmanlamaya öncelik vermektedir. Bununla birlikte, Mykolas Romeris Üniversitesi, dinamik teknolojik bağlamlarda stratejik yönetime güçlü bir vurgu yaparak, modern BT ortamlarını ve karmaşık siber güvenlik görevlerini denetlemede usta uzmanlar üretmeyi amaçlayan, siber güvenlik yönetimine belirgin bir şekilde eğilmektedir.

Lisans düzeyindeki siber güvenlik çalışma programları, bilişim ve siber güvenlik alanında yetenekli profesyoneller geliştirmeye odaklanır, ancak her biri farklı vurgulara sahiptir. Vilnius Üniversitesi'nin programı, güvenli bilgi sistemlerinin analizi, tasarımı, geliştirilmesi ve bakımına odaklanarak bilişim mühendisliğinde kapsamlı bir temel sağlamaya yöneliktir. Marijampole College, aynı zamanda yetkin bilişim uzmanları yetiştirmeyi hedeflerken, bilgisayar ağları ve sistemleri oluşturma, sürdürme ve yönetme gibi pratik yönlere daha fazla önem vermektedir. Kaunas College, yalnızca siber sistemleri tasarlama ve uygulama konusunda değil, aynı zamanda ekiplere liderlik etme, etik, yasal ve sosyal sonuçları anlama ve çok kültürlü ortamlarda etkin bir şekilde çalışma becerisine sahip uzmanlar hazırlamayı hedefleyerek kendini farklılaştırmaktadır. Her üç kurum da öğrencileri siber güvenlik alanında teknik becerilerle donatmayı amaçlarken, hedefleri teknik yeterlilikten (Vilnius Üniversitesi), pratik uygulama ve sosyal beceri geliştirmeden (Marijampole Koleji), teknik, liderlik ve etik hususların bir karışımına (Kaunas Koleji) kadar çeşitlilik gösterir

Araştırma ayrıca, siber güvenlik alanında, her biri, özellikle kriptografi kullanarak siber saldırıları tanımak, araştırmak ve önlemek için gerekli becerilere odaklanan dört kayıtlı yaygın yetişkin eğitimi programını ortaya çıkardı. Tüm programlar bu temel hedefi paylaşsa da, yaklaşımları ve kapsamları farklıdır. Bazıları siber güvenlik ve önleyici stratejilere odaklanırken, diğerleri sosyal mühendislik, kimlik yönetimi ve risk yönetimi gibi alanları kapsayan programlama dahil daha geniş bir müfredat sunar. Özellikle, birkaç program temel programlama ile başlar ve yeni başlayanlar için uygun olan gelişmiş siber güvenlik konularına ilerler. Cybint ile işbirliği içinde öne çıkan bir program, hem tam zamanlı hem de yarı zamanlı formatlarda pratik, gerçek dünya becerileri sunarak sınırlı BT bilgisine sahip olanlara hitap ediyor. Bu programlar toplu olarak, temel programlamadan derinlemesine, uygulama odaklı öğrenmeye kadar çeşitli siber güvenlik yetkinlikleri geliştirmeyi amaçlamaktadır.

Finlandiya'nın ulusal güvenliğini ve savunmasını güçlendirmeye yönelik çeşitli politikalar, siber güvenlikle ilgili eğitim programlarını etkilemiştir. Siber güvenlik alanında artan sayıda araştırma ve geliştirme girişimi, eğitim ve öğretim programı ve sertifikalı profesyonel bulunmaktadır. Finlandiya Siber Güvenlik Stratejisi (2019) (**https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/**) ve Siber Güvenlik Geliştirme Programı (2021), eğitim ve araştırma yoluyla ulusal siber güvenlik yetkinliği oluşturmanın önemini vurgulamaktadır. Okul eğitim sistemi için amaç, öğrencileri dijital dünyada güvenli bir şekilde gezinmek için bilgi ve becerilerle donatmak ve siber tehditler ve korunma önlemleri konusunda farkındalık **Lehto-IWS-018.pdf (jyu.fi)**

Finlandiya Mesleki Eğitim ve Öğretim'de (MEÖ) siber güvenlik, çoğu materyalde ayrı veya özel bir odak noktası olarak açıkça vurgulanmamıştır. Ancak bu, siber güvenliğin Mesleki Eğitim ve Öğretim programlarında tamamen bulunmadığı anlamına gelmez. Tüm sektörlerde dijital okuryazarlık ve siber güvenliğin artan önemi göz önüne alındığında, bu konular daha geniş BT ve teknik eğitim programlarına entegre edilmiştir. Finlandiya'daki Mesleki Eğitim ve Öğretim sağlayıcılarının eğitim tekliflerini bölgesel ve alana özgü gereksinimlere göre düzenleme özerkliğine sahip olduğunu belirtmek önemlidir. Finlandiya'da mesleki eğitim ve öğretim son 20 yılın en kapsamlı reformunu gerçekleştirmiştir. 2018 reformunun amacı, daha verimli ve esnek, yetkinlik temelli ve müşteri odaklı bir Mesleki Eğitim ve Öğretim sistemi oluşturmak, verimliliğini artırmak ve nitelikleri işgücü piyasası ihtiyaçlarına daha iyi uydurmaktı. Bu, esas olarak düzenlemeyi azaltarak ve Mesleki Eğitim ve Öğretim sağlayıcıları için daha fazla özerklik ve sorumluluk getirerek yapılır. (Kaynak: **https://www.cedefop.europa.eu/files/8133_en.pdf)** Bu, bazı kurumların yerel endüstri taleplerine ve ortaklıklarına bağlı olarak siber güvenlik gibi alanlarda daha özel modüller sunabileceği anlamına gelir. Lehto'nun araştırmasına göre, siber güvenlik ayrı bir konu değil, özellikle Bilgi ve İletişim Teknolojileri (BİT) bağlamında farklı konulara entegre edilmiştir. Öğretimin sorumluluğu, öğretmenlerin siber güvenlik eğitimini derslerine dahil etmelerine bağlıdır. Bu yaklaşım, bunun farklı okullar ve sınıflar arasında nasıl uygulandığı konusunda bir çeşitliliğe yol açmakta ve potansiyel olarak ayrı bir konu veya BİT eğitiminin daha belirgin bir parçası haline getirmek de dahil olmak üzere, siber güvenliği öğretmek için daha yapılandırılmış ve tutarlı yaklaşımlara duyulan ihtiyacı vurgulamaktadır.

Yüksek Öğrenim (HE) düzeyinde, Fin üniversiteleri kapsamlı Siber Güvenlik lisans programları sunmaktadır. Bu programlar, öğrencileri siber güvenliğin çeşitli alanlarında ileri düzeyde bilgi ve becerilerle donatmak için tasarlanmıştır. Birçoğu, bu kavramların gerçek dünyadaki etkilerine ve uygulamalarına odaklanan bilgi güvenliği ve bilgi teknolojisi alanında yüksek lisans derecesi sunar. Bunlara yerinde ve uzaktan erişilebilir.

Belçika'daki siber güvenlik sektörü, yaklaşık 4.000 açık siber güvenlik açık pozisyonuyla (Kasım 2022 itibariyle) vasıflı profesyoneller için artan bir talep yaşıyor. Bu boşluğu doldurmanın aciliyetini ve ihtiyacını kabul ederek, ülkenin siber güvenlik uzmanlığını geliştirmek için çeşitli girişimler ve eğitim programları başlatıldı. Belçika'da KU Leuven, Solvay Business School, Howest University of Applied Sciences ve diğerleri gibi çok sayıda kurum, geniş bir kitleye ulaşabilen İngilizce, Fransızca ve Felemenkçe dillerinde özel programlar geliştirmiştir. Bununla birlikte, Belçikalı kuruluş Agoria tarafından yürütülen araştırma, siber güvenlik alanı ve tehditleri hakkında güncel kalmaları için artık üniversiteye gitmeyen profesyoneller arasında da sürekli eğitim ihtiyacını vurguladı. 2021-2025 yılları için Belçika Siber Güvenlik Stratejisi, siber güvenliğin ülkenin akademik ortamına yüksek düzeyde entegrasyonunu kabul ediyor ve üniversitelerin ve diğer eğitim kurumlarının bu alandaki araştırma ve geliştirme çabalarını artırmada oynadığı önemli rolün altını çiziyor. CBB'nin (Belçika Siber Güvenlik Merkezi) veritabanına göre, Belçika'da, Yüksek Öğretim Kurumları tarafından sunulan ve hem kamu hem de özel sektörde sunulan bir dizi Mesleki Eğitim ve Öğretim programına ek olarak sunulan 33 kurs (lisans, yüksek lisans ve sertifikalar) bulunmaktadır. CBB, Belçika siber güvenlik stratejisinin uygulanmasını denetleyen, koordine eden ve izleyen bir organdır ve şu anda Belçikalı çalışanlar için siber güvenlik bilgisini nüfus arasında daha da fazla yaymak için ücretsiz bir Çalışan Siber Güvenlik

Farkındalık Eğitimi geliştirmektedir. Genel olarak, Belçika siber güvenlik stratejisi, siber güvenlik bilgi ve becerilerinin eğitim yoluyla yayılmasının önemini vurguluyor ve akademik kursları genişletmeyi, bu alandaki araştırmaları teşvik etmeyi, STEM eğitimini teşvik etmeyi ve Belçika siber güvenlik ortamındaki profesyonellere yönelik artan talebi karşılamak için pratik eğitim fırsatları sağlamayı taahhüt ediyor.

Norveç'te Siber güvenlik, Mesleki Eğitim ve Öğretim düzeyinde çalışılabilecek ana konu değildir. Programın unsurları "Bilgisayar ve Elektronik" adlı bir Mesleki Eğitim ve Öğretim programına dahil edilmiştir. Siber güvenlik için eğitim bakanlığı çerçevesi yoktur, yalnızca tüm eğitim için genel temel dijital okuryazarlık becerilerinde, öğrencilerin ağların içinde ve dışında dijital kaynakları kullanabilmeleri ve gezinebilmeleri ve bilgi ve veri güvenliğini koruyabilmeleri gerektiğinden bahseder.

Ulusal Siber Güvenlik Yetkinlik Stratejisi , 14 Kasım 2023'te Mesleki Eğitim ve Öğretim okulu öğrencilerinin siber güvenlik hakkında bilgi edinmelerinin önemine işaret ediyor. Birçok mesleki konu için bu çok alakalı ve önemlidir. Mesleki kurslarda siber güvenlik öğrenme materyallerinin eksikliği vardır ve öğretmenler, özellikle gizlilik, akıllı ev teknolojisi ve IoT gibi alanlarda öğretme becerilerinden yoksundur. GenCyber ve CyberFirst gibi siber güvenlik eğitimi için mevcut programlar, bu mesleki programın ihtiyaçlarını özel olarak ele almamaktadır. (**kaynak 1 – 2**)

UiO, NTNU ve seçilen Mesleki Eğitim ve Öğretim okullarındaki öğretmenler arasındaki işbirliği sayesinde, plan, daha sonra ulusal öğrenme platformu NDLA'da **(Ulusal Dijital Öğrenme Arenası) kullanıma sunulacak olan siber güvenlik için öğrenme materyali geliştirmektir**.

Yüksek öğrenimde, hem Dijital güvenlik kültüründe bir yıllık program hem de siber güvenlik alanında lisans programları bulabilirsiniz. Konu ayrıca Veri Bilimleri ve Bilişim alanında bir dizi yüksek lisans programında da yer almaktadır. Uygulamalı bilgisayar ve bilgi teknolojisi, Siber Güvenlik Lisansı, Dijital Adli Tıp Lisansı, Dijital altyapı ve siber güvenlik, Dijital güvenlik kültürü ve bilgi güvenliğinde deneyime dayalı yüksek lisans gibi çeşitli özel siber güvenlik çalışmaları vardır. Siber güvenliğin SEÇ kültürü ve liderliği olarak yer aldığı çalışmalar, uygulamada belediye acil durum hazırlık kooperatifleri ve yönetim kurulu çalışmaları ve kriz yönetiminde yıllık çalışmalar da bulunmaktadır.

Polonya için son yıllarda siber çalışmalar artmıştır. Üniversitelerde giderek daha fazla siber kurs açılıyor ve aynı zamanda Mesleki Eğitim kurslarının sayısı artıyor. Polonya'da son yıllarda siber mesleklere olan talep arttı ve şirketleri siber uzmanları istihdam etmeye ve bilgileri korumaya teşvik eden Polonya heyetinde siber farkındalık da arttı.
Polonya'da, çoğu Avrupa ülkesinde olduğu gibi, akademik bir derece zorunlu kabul edilir ve bu nedenle siber kurslar genellikle dereceden sonra ek bir çalışmadır. Çünkü Akshmi çalışmalarının çoğu daha uzun ama teorik bir şekilde. Kısa siber kurslar var, ancak çoğu gerçek çalışmaya hazırlayan pratik öğrenmeye odaklanıyor. Siber alandaki bir öğrenci için en büyük zorluk, Mesleki Eğitim kurumlarının çoğunun kendi fonlarına sahip olmamasıdır, bu nedenle finansal bir çözüm gereklidir ve bu nedenle bu seçenek ilgilenenler için her zaman uygun değildir.

Siber güvenlik tüm faaliyet alanları için bir öncelik olsa bile, Romanya'daki Mesleki Eğitim ve Öğretim eğitim sistemi, öğrencilerin bu alanda yetkin olmalarını sağlamaya henüz hazır değildir. Herhangi bir mesleki eğitim alanında, lisenin alt döngüsü - teknolojik alan - için Müfredatın analizinde, teknik kültür için okul müfredatı, siber güvenlikle ilgili öğrenme çıktıları birimleri sağlamaz. Alandaki bazı özel yeterlilikler genel kültür müfredatında, Bilgi ve İletişim Teknolojileri disiplininde, 9. sınıf müfredatında bulunabilir. Bunlar:

1. İnternet kullanımında güvenlik önlemlerinin tanımı ve uygulanması:

- İnternetin akıllı kullanımı
- Veri iletim şifrelemesinin önemi
- Dijital imza kullanımı
- Virüslere karşı korunma yolları

2. Sohbet servisini kullanma:

- Video konferans için işbirlikçi uygulamaların sunumu
- IRC ağ kurallarının sunumu

Lisenin üst kademesi için, 11. sınıflar için sadece mesleki eğitim alanı olan Elektronik Otomasyon uzmanlıkları için Telekomünikasyon Teknikeri, Bilgisayar Operatörü Teknisyeni, Telematik Operatör Teknisyeni, Güvenlik Uygulamalarının Kurulumu ile ilgili bazı içerikler sunmaktadır. 12. sınıfta, yalnızca Bilgisayar Teknisyeni uzmanlığında, özel modül aşağıdaki gibi içerikleri içerir:

- Bilgisayar sistemlerinin ve bilgisayar ağlarının güvenliğinin temel ilkeleri
- Ağda güvenlik politikalarının geliştirilmesi
- Ağların güvenlik tehditleri
- İnternette gezinme koruması
- Virüsler ve güvenlik uygulamaları

HEI ile ilgili olarak, Brasov Transilvania Üniversitesi, siber güvenlik eğitimine güçlü bir bağlılık göstermekte ve tamamen İngilizce olarak yürütülen Siber Güvenlik alanında kapsamlı bir Yüksek Lisans programı sunmaktadır. Üniversitenin bu kritik alanda uzmanlığı geliştirmeye olan bağlılığı, program için sağlanan kapsamlı müfredatta açıkça görülmektedir.

Transilvania Üniversitesi'ndeki bu yüksek lisans programı, uluslararası bir akademik ortamda siber güvenlik alanında çok yönlü bir eğitim arayan öğrenciler için mükemmel bir fırsattır. Sağlam bir müfredat ve İngilizce eğitiminin birleşimi, mezunları dinamik ve zorlu siber güvenlik alanında başarı için konumlandırır.

Cluj-Napoca'daki Babes-Bolyai Üniversitesi, Matematik ve Bilişim Fakültesi aracılığıyla, 2023-2024 akademik yılından itibaren Siber Güvenlik alanında İngilizce yüksek lisans programı başlattı ve bu alanda geleceğin uzmanlarını hazırlamayı amaçladı. Yeni programın dersleri bu yıl Ekim ayında başlıyor, 2023-2024 akademik yılı ile birlikte kabul, beklentilerin ötesinde bir rekabet getiriyor. Programa kabul edilen yurt dışından da dahil olmak üzere 40'tan fazla öğrenci

Siber Güvenlik alanında uzman olacak, kabul edilen adaylar Avrupa'daki diğer ünlü üniversitelerde bir akademik yıl okumayı bile seçebilirler.

Matematik ve Bilgisayar Bilimleri Fakültesi'nde *İnternet Teknolojileri* Yüksek Lisans Programı (İngilizce) ayrıca birinci yılın ikinci döneminde, *öğrencilere Siber Güvenlik alanını ve belirli veri şifreleme yöntemlerini tanıtan* Kriptografi ve Sistem Güvenliği dersi sunmaktadır.

Ayrıca, Yazılım Sistem Mühendisliğinde Modern Teknolojiler Yüksek Lisans Programı, ikinci yılın ilk döneminde, siber güvenliğin temel zorluklarına odaklanan BT sistemleri güvenliği adı verilen isteğe bağlı bir ders sunmaktadır.

Her iki ders de Matematik ve Bilişim Fakültesi'ndeki yüksek lisans öğrencilerinin, gerçek uluslararası bağlamda hayati öneme sahip olan bu konuda içgörü ve uzmanlık kazanmalarına ve modern sistemlerin şifreleme ve güvenlik zorluklarının farkına varmalarına olanak tanır.

Bükreş Üniversitesi, Matematik ve Bilişim Fakültesi, kriptografi ve sistem güvenliğine adanmış bir dizi kurs sunan bir Güvenlik ve Uygulamalı Mantık Yüksek Lisans Programı (İngilizce) sunmaktadır. Öğrenciler, işletim sistemi güvenliği, kriptografi, ağ güvenliği ve siber güvenlik alanlarında bilgi edinebilir ve böylece bu alanın zorluklarıyla yüzleşmeye hazır olabilirler.

İspanya'da siber güvenlik alanındaki çalışmaların çoğu Yüksek Öğrenim Düzeyi, derece veya yüksek lisans derecesindedir. İspanya Ulusal Siber Güvenlik Enstitüsü tarafından kurtarılan verilere göre:

- Devlet ve özel üniversiteler ve diğer yüksek öğretim kurumları tarafından sunulan siber güvenlik alanında yaklaşık 87 yüksek lisans derecesi.
- 4 uzmanlık, çoğunlukla adli bilişim uzmanlığı.
- Hepsi özel sektör tarafından sunulan 3 üniversite diploması.

Mesleki Eğitim ve Öğretim düzeyinde eğitime gelince, İspanyol mesleki eğitim enstitülerinde yaklaşık 60 kurs bulunmaktadır. Hepsi, Mayıs 2020'de Milli Eğitim Bakanlığı tarafından 7 *Nisan tarihli 479/2020 sayılı Kraliyet Kararnamesi ile onaylanan ve bilgi teknolojisi ortamlarında siber güvenlik konusunda uzmanlık kursunu belirleyen* aynı müfredatla düzenlenir.

Mevcut programlara rağmen, daha fazla çabaya ihtiyaç duyulduğu kabul edilmektedir. İspanya, Ulusal Dijital Beceriler Planı, KOBİ Dijitalleşme Planı 2021-2025 ve İspanya Dijital 2025 Planı dahil olmak üzere, özellikle siber güvenlik alanında dijital becerilere yönelik artan talebi karşılamak için yeni yetenekler yaratmaya odaklanan çeşitli planlar uyguladı.

Türkiye'de siber güvenliğe olan ihtiyaç hızla artmış ve özellikle son yıllarda tüm dünyada olduğu gibi ülkemizde de oldukça önemli bir hale gelmiştir. Teknolojik gelişmelerle eş zamanlı olarak siber riskler ve tehditler de aynı hızla değişmiş ve karmaşık hale gelmiştir. Siber risk ve tehditler, fiziksel saldırılardan çok daha kapsamlı ve olumsuz sonuçlar doğurma potansiyeline ulaşmıştır. Finans, elektronik haberleşme, enerji, ulaştırma ve havacılık gibi sektörlerin güvenli dijital ortamda hizmet sunması ile ulusal siber güvenliğin sağlanması ülkemiz için en önemli önceliklerden biri haline gelmiştir. Bu kapsamda, sektörün ihtiyaçları doğrultusunda mesleki

eğitim ve yükseköğretimde siber güvenlik eğitimlerinin yaygınlaştırılması ve eğitim içeriklerinin geliştirilmesi ve zenginleştirilmesi için çalışmalar devam etmektedir.

Bu çalışmalar kapsamında mesleki eğitimde: Bilişim teknolojileri alanında ağ işletiminde siber güvenlik temelleri dersi. Siber güvenlik alanında, programlama temelleri, sistem güvenliği, ağ teknolojileri, güvenli yazılım geliştirme, sızma testi ve siber olaylara müdahale, adli bilişim vb. Ders kazanımları öğrencilere verilir.

Yükseköğretimde, siber güvenlik meslek yüksekokullarında "Siber Güvenlik Analisti ve Operatörü" ön lisans programı, üniversitelerde Adli bilişim mühendisliği lisans programı ve üniversitelerde ilgili yüksek lisans programları sunulmaktadır.

Ayrıca üniversitelerin sürekli eğitim merkezleri, belediyelerin halk eğitim merkezleri, TÜBİTAK, TSE gibi resmi kurumlar ve özel eğitim kurumları da siber güvenlik konusunda eğitimler vermektedir.

2.1.2. SIBER GÜVENLIK ZORLUKLARI VE SEKTÖR IHTIYAÇLARI

Kapsamlı bir literatür taramasına dayanarak, projenin ülkelerindeki KOBİ'lerin karşılaştığı siber güvenlik zorluklarını listeledik. Gelişen siber güvenlik ortamında, Litvanya'daki küçük ve orta ölçekli işletmeler (KOBİ'ler) birden fazla siber güvenlik sorunuyla karşı karşıyadır. Bu işletmeler, operasyonları için dijital teknolojilere giderek daha fazla güvendikçe, bir dizi siber tehdide karşı daha savunmasız hale geliyorlar ve bu riskleri etkin bir şekilde yönetmek için kapsamlı bir anlayış ve stratejik yaklaşım gerektiriyor.

2022 çalışmasında Bukauskas ve ark.[8] Siber güvenlik olgunluklarına ve yetkinlik ihtiyaçlarına göre seçkin kuruluş türleri. Araştırmaya göre, dijital çalışma alanı güvenliğinin ana parametresi, siber güvenlik tehditlerinin genel anlayışından etkilenen siber hijyen düzeyi olduğundan, küçük kuruluşlar toplumdaki bireysel kişilerle karşılaştırılabilir. Bu katmanda siber güvenlik, kuruluş içinde dahili olarak koordine edilir ve iş süreçlerinde potansiyel güvenlik ihlallerine yol açar. Orta ölçekli şirketlerde, siber güvenliğin yönetimi ve düzenlenmesi de zayıf bir şekilde koordine edilmektedir. Olaylara veya diğer siber güvenlik faaliyetlerine verilen yanıtlar da kuruluş içinde vurgulanmaz. Litvanya'daki küçük işletmelerin tüm şirketlerin %97'sini oluşturduğunu akılda tutan Bukauskas ve ark. (2022), BT hizmetleri sağlayan, kullanıcılara danışan ve iş işlevleri temel siber güvenlik ilkelerini sağlamayı içeren BT uzmanlarına önemli bir ihtiyaç olduğu sonucuna varmıştır. Ayrıca, tehdit istihbaratı ve bilimsel araştırmalarda kayda değer bir eksikliğin gözlemlendiğini ve güvenlik mühendisliği ve sistem yaşam döngüsünde siber güvenlik uzmanlarına gözle görülür bir ihtiyaç olduğunu vurguladılar.

Birkaç yıl önce, "Litvanya için Yarat" programı, Milli Savunma Bakanlığı ile işbirliği içinde, küçük ve orta ölçekli işletmeler arasında siber güvenlik bilincini artırmaya yönelik bir kamuoyu

[8] Bukauskas, L., Brilingaitė, A., Lepaitė, D., Juozapavičius, A., Ikamas, K., 2022. 'Projekto "Kibernetinio saugumo kompetencijų žemėlapio kūrimas" ataskaita', Vilniaus universitetas Informatikos institutas. Şu adresten ulaşılabilir: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf [Erişim tarihi: 12 Ocak 2024]. DOI: https://doi.org/10.15388/CIBERSEK.2022.

istişaresini düzenledi[9]. Girişim ayrıca, Litvanya'daki KOBİ'ler arasında siber güvenlik farkındalığı düzeyinin yüksek olmadığı ve küçük işletmelerin dijital risklerin anlaşılmaması nedeniyle yeterli düzeyde siber dayanıklılık elde edemediği sonucuna vardı. Ayrıca girişim, şirket liderlerinin yarısından fazlasının (%57) siber güvenlik çözümlerini seçmek için yeterli bilgiye sahip olmadıklarını veya emin olmadıklarını belirttiğini ve çalışanların dörtte üçünden fazlasının kolay anlaşılır bilgilerden yoksun olduklarını kabul ettiğini belirtti.

Bukauskas ve ark. (2022) ve daha önceki "Create for Lithuania" (2019) girişimi, Litvanya'daki KOBİ'ler arasında siber güvenlikle ilgili durumun sınırlı ilerleme gösterdiği açıktır. Her iki çalışma da bu işletmelerde temel siber güvenlik bilgisi ve hazırlığı konusunda kalıcı bir eksikliğin altını çiziyor. Dijital teknolojilere olan güvenin artmasına rağmen, KOBİ'ler yetersiz siber dayanıklılık ve dijital risklerin genel olarak anlaşılmaması nedeniyle güvenlik açıkları sergilemeye devam ediyor. Devam eden bu zorluk, Litvanya'nın iş ortamının çoğunluğunu oluşturan kritik bir sektör olan KOBİ'ler arasında gelişmiş siber güvenlik farkındalığı ve eğitimine yönelik acil ihtiyacı vurgulamaktadır.

Finlandiya'da, Finlandiya Ekonomik Araştırma Enstitüsü ETLA (Elinkeinoelämän tutkimuslaitos) tarafından yapılan bir araştırma, KOBİ'ler de dahil olmak üzere Fin şirketlerindeki veri ihlallerinin sayısının iki yılda iki katına çıktığını vurguladı. Finlandiyalı şirketler, 2019'da Avrupa ortalamasından üç kat daha fazla veri ihlali bildirdi ve çoğu olay dolandırıcılık, kimlik avı saldırıları, veri ihlalleri, kötü amaçlı yazılımlar ve güvenlik açıklarıyla ilgiliydi. Bu çalışma aynı zamanda Fin KOBİ'leri için ana zorluk olarak yetenekli siber güvenlik uzmanlarının eksikliğini de vurgulamaktadır. **https://www.etla.fi/en/publications/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/**

Finlandiya Ulusal Siber Güvenlik Merkezi (NCSC-FI) (**https://www.kyberturvallisuuskeskus.fi/en**), Finlandiya hükümeti tarafından yönetilen bir girişimdir. Finlandiya'da iletişim ve ulaştırma sektörlerinin düzenlenmesinden sorumlu bir devlet kurumu olan Finlandiya Ulaştırma ve İletişim Ajansı'nın (Traficom) bir parçası olarak faaliyet göstermektedir. Siber güvenliğin mevcut durumu hakkında bilgi sağlarlar ve hem bireylere hem de kuruluşlara siber güvenlik uygulamalarını geliştirmeleri için rehberlik ve araçlar sunarlar. Merkez ayrıca güvenlik açığı uyarıları gibi ulusal siber güvenlik girişimlerinde bulunur ve siber tehditlere karşı farkındalığı ve hazırlığı teşvik eder.

Haftalık incelemeleri, KOBİ'lerin karşılaştığı zorluklar hakkında iyi bir fikir veriyor. Finlandiyalı KOBİ'lerin, diğerleri gibi, birçok kimlik avı ve dolandırıcılık mesajı tarafından hedef alınma konusunda ETLA enstitüsü tarafından açıklanan aynı güvenlik sorunlarıyla karşı karşıya kaldığını öğreniyoruz. Bunlar, kimlik bilgileri veya diğer hassas bilgiler için kimlik avı Suomi.fi gibi meşru hizmetlerin kimliğine bürünme girişimlerini içerir. KOBİ'lerin finansal kaynakları, siber tehditlere karşı savunmak için modern siber güvenlik çözümlerini dağıtmak için bir sınırlama olabilir. Aynı tarafta, halihazırda donanımlı olan KOBİ'ler, ortaya çıkan siber güvenlik tehditlerine karşı güncel kalmakta zorlanıyor.

[9] Litvanya ve Milli Savunma Bakanlığı için oluşturun, 2019. SVV Kibernetinio Saugumo Apklausos Apžvalga. [çevrimiçi] Mevcut: http://kurklt.lt/wp-content/uploads/2019/12/SVV-kibernetinio-saugumo-apklausos-ap%C5%BEvalga-Kurk-Lietuvai.pdf

Belçika'daki KOBİ'lerin karşılaştığı siber güvenlik durumunu anlama çabamızda kapsamlı bir araştırma yaptık. Ancak, bu kritik sorunu ele alan kapsamlı veriler veya kaynaklar elde etmekte zorlandık. Bu bilgi eksikliği, KOBİ'lerin dijital varlıklarını siber tehditlere karşı korumalarına yardımcı olabilecek etkili stratejiler ve çözümler oluşturmayı zorlaştırıyor.

Women4Cyber Vakfı'nın geniş ağı sayesinde Belçika'da siber güvenlik alanında aktif olarak yer alan profesyonellere ulaşabildik. Bu uzmanlar bize, KOBİ'lerin siber güvenlikte karşılaştıkları çeşitli zorlukları anlamamıza yardımcı olan hayati içgörüler ve bakış açıları sağladı. Women4Cyber Belgium'un önemli bir üyesi olan Iva Tasheva'dan, KOBİ'lerin dijital altyapılarını siber tehditlerden korumaya çalışırken karşılaştıkları zorluklar hakkındaki kapsamlı deneyim ve bilgilerini paylaşan içgörüler aldık.

KOBİ'ler, geçici desteğe erişimde zorluklar, personeli için Kimlik ve Erişim Yönetimi eğitiminin olmaması ve bulut hizmetleri rollerinin ve sorumluluklarının sınırlı anlaşılması gibi çeşitli siber güvenlik zorluklarıyla karşı karşıyadır. Ek olarak, KOBİ'lerin uygun fiyatlı güvenlik açığı tarama çözümlerine ve izleme araçlarına sınırlı erişimi vardır ve bu da onları siber tehditlere karşı daha savunmasız hale getirir. İş ortamlarındaki yaygın hiper bağlantı, KOBİ'leri kimlik hırsızlığına ve dolandırıcılık faaliyetlerine maruz bırakırken, kimlik avı ve dolandırıcılık devam eden riskler oluşturur. Bu zorlukların üstesinden gelmek için KOBİ'lerin proaktif önlemler alması, sağlam güvenlik protokolleri uygulaması ve becerilerini güçlendirmek ve olası ihlallere ve mali kayıplara karşı korunmak için kapsamlı çalışan eğitimi sağlaması gerekir.

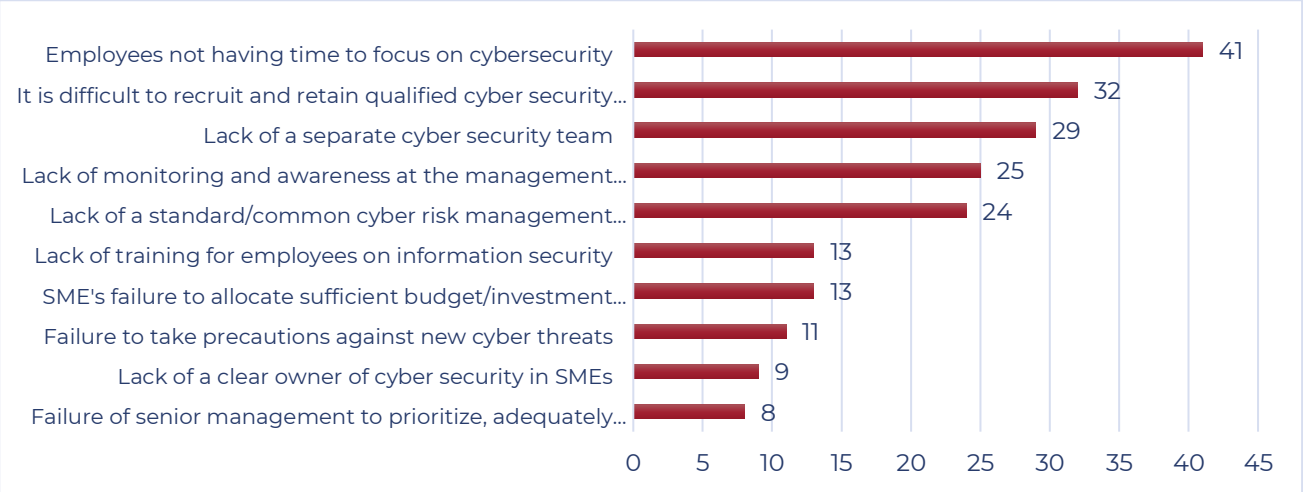
Siber güvenlik, küçük ve orta ölçekli işletmeler (KOBİ'ler) dahil olmak üzere İspanya'daki işletmeler için en önemli önceliklerden biri haline geldi. Uzaktan çalışma ve çevrimiçi derslerdeki artış, diğerlerinin yanı sıra uzak masaüstü işlevlerinin, bulut bilişimin ve işbirlikçi araçların yaygın olarak kullanılmasına, risklerin ve bilgisayar saldırılarının artmasına neden oldu. Ulusal Kriptoloji Merkezi (CCN-CERT) tarafından hazırlanan rapor, uzaktan çalışma ve teknoloji kullanımındaki artışı bu risklerdeki artışla ilişkilendiriyor. Şirketlerin en sık maruz kaldığı saldırılar fidye yazılımı ve uzaktan erişim sistemlerine yapılan saldırılardır. Siber tehditlerin artması, şirketlerin siber güvenlik ekiplerine dahili veya harici olarak atanan kişi sayısını artırmasına neden oldu. Ancak buna rağmen, şirketler hala bu işlevlerin yaklaşık %50'sini dışarıdan temin ediyor.

Buna ek olarak, İspanya'da hala olayları işlemek için Güvenlik Operasyon Merkezlerine (SOC) sahip olmayan şirketlerin %21'i var. İş ortamında siber güvenlik eğitimi açısından, Deloitte'un analizi, 2022'de analiz edilen kuruluşların çalışanları için siber güvenlik konusunda çevrimiçi eğitim saatlerinin 2021 verilerine kıyasla neredeyse %30 arttığını vurguluyor. Bununla birlikte, İspanya'daki şirketlerin neredeyse %50'sinin siber güvenlik konusunda herhangi bir sertifikası yoktur ve bu da gelecek için açık bir zorluktur.

Bununla birlikte, İspanyol şirketlerinin karşılaştığı en büyük zorluk hala siber güvenlik alanındaki yetenek eksikliğidir. ObservaCiber tarafından hazırlanan "İspanya'da Siber Güvenlik Yeteneğinin Analizi ve Teşhisi" raporuna göre, 2021'de İspanya'da 24.119'da tahmin edilen bir yetenek açığı

vardı. 2024'te İspanya'nın 83.000'den fazla uzmana ihtiyaç duyacağı ve yetenek açığını %57,5'e çıkaracağı tahmin ediliyor.

KOBİ'lerin siber güvenlik sorunlarıyla karşılaşmasına neden olan en zayıf halkanın "insan" faktörü olduğu görülüyor. KOBİ'ler için en büyük zorluk, siber güvenlikten sorumlu personelin birden fazla alanda sorumlulukları olduğu için siber güvenlik alanına yeterli zaman ayıramamasıdır. Bununla bağlantılı olarak ayrı bir siber güvenlik ekibinin olmaması, KOBİ'lerin siber güvenlik yönetiminde yaşadığı zorluklar listesinde üçüncü sırada yer alıyor. KOBİ'ler, nitelikli siber güvenlik çalışanlarını işe alma ve elde tutma konusunda sorun yaşıyor.



Şekil 1 - KOBİ zorlukları - Türkiye araştırması.

Romanya'da çevrimiçi ortam, KOBİ'lerin gelişmesine yardımcı olabilecek iş fırsatları ve bağlantılar getiriyor, ancak aynı zamanda birçok risk de içeriyor.

Siber güvenlik artık bir hikaye değil, Romanya'da da bir gerçek, şimdiye kadar büyük bir siber saldırı yaşamamış olsak bile.

Kullanılan bilgi kaynağı, 5.199'u veri güvenliği ihlali olarak doğrulanan 16.312 güvenlik olayına dayanan KOBİ'ler için ana kilit noktalar olan 2023'teki siber tehditlere ilişkin VERIZON RAPORU'dur (VERİ İHLALI ARAŞTIRMALARI RAPORU - DBIR).

KOBİ'ler için ilgi noktaları:

- KOBİ'ler ve şirketler için saldırı yüzeyleri benzerdir, çünkü bulut tabanlı yazılım kullanırlar. Sisteme yetkisiz sızma, sosyal mühendislik teknikleri ve temel web uygulaması saldırıları, KOBİ'ler tarafından kaydedilen ihlallere yönelik toplam saldırı türlerinin %92'sini temsil etmektedir (kurumlar için %85).
- Fidye yazılımı vakaların %24'ü (veriler şifrelenmeden önce çalınır)
- Sisteme yetkisiz sızma - hedeflerine ulaşmak için kötü amaçlı yazılımlara ve/veya bilgisayar korsanlığına dayalı karmaşık saldırılar.

- Dış saldırganlar, mevcut güvenlik ihlallerinin %83'üne neden olan en büyük tehdidi temsil ediyor ve KOBİ saldırıları durumunda %94'e ulaşıyor. Tehditlerin yayılmasına dahil olan aktörlerin %94'ü, büyük kuruluşlarda %89'a kıyasla dışarıdadır ve ihlallerin %98'i, şirketler söz konusu olduğunda %97'ye kıyasla finansal olarak motive edilmiştir.
- Finansal motivasyon tüm vakaların %95'inde bir numaradır, KOBİ'lere yönelik saldırılarda bu oran %98'e çıkmaktadır. Sadece% 1'i casusluk tarafından motive ediliyor.
- Çalışanlar güvenlik zincirindeki zayıf halkayı temsil ediyor - tüm vakaların %74'ü (siber tehditler konusunda zayıf farkındalık). İzinsiz girişin ana yöntemi, çalınan kimlik bilgilerinin -% 49 ve% kimlik avı,% 12 veya yanlış yapılandırma veya hassas verilerin hatalı gönderilmesi gibi diğer yöntemlerin kullanılmasından kaynaklanabilir.
- İş e-postalarını tehlikeye atmak - kurban, saldırganların hesaplarına büyük miktarda para aktarması için kandırılır.

Norveç'te küçük ve orta ölçekli işletmeler (KOBİ'ler) siber güvenlik konusunda önemli zorluklarla karşı karşıyadır. Birçoğu, potansiyel güvenlik açıklarına yol açan riskler hakkında derin bir anlayıştan yoksundur. Siber güvenlik konusunda etkili çalışan eğitiminde gözle görülür bir boşluk var ve bu da insan hatasını yaygın bir risk faktörü haline getiriyor. KOBİ'ler, özellikle sınırlı kaynaklara sahip olduğunu bildirenler, genellikle gelişmiş siber güvenlik önlemlerine ve vasıflı personele yatırım yapmakta zorlanıyor. Ayrıca, hassas bilgileri korurken uyumluluğu sağlamanın karmaşıklığını artıran karmaşık veri koruma yasalarında gezinmeleri gerekir. Kimlik avı saldırılarındaki ve sosyal mühendislikteki artış, yetersiz ağ güvenliği ve iç tehdit riski gibi güvenlik açıklarını daha da gösteriyor. Bu risklerin yönetilmesi kritik öneme sahiptir, ancak KOBİ'ler genellikle etkili risk değerlendirmesi ve yönetimini zor bulmaktadır. Ek olarak, üçüncü taraf satıcılara güvenmek, KOBİ'leri potansiyel olarak ek siber güvenlik tehditlerine maruz bırakan başka bir karmaşıklık katmanı sunar.

2.2. SIBER GÜVENLIKTE KADINLAR

Kadınlara yönelik eğitim ve destek ihtiyaçlarını, kadınların siber güvenlik alanındaki mevcut niteliklerini ve yetkinliklerini analiz ettik ve siber güvenlik zorluklarına daha fazla kadın çalışanı dahil etmek için öneriler sunduk.

Microsoft, 35 Avrupa ülkesinde bir anket yaptı, bilgisayar bilimleri mezunlarının 5'te 1'inden azı kadındı. Bilim, teknoloji, mühendislik ve matematiğe (STEM konuları) olan ilgi çok erken düşüyor. Aslında, OECD'nin Uluslararası Öğrenci Değerlendirme Programı (PISA), erkeklerin kendilerini BİT uzmanları, bilim adamları veya mühendisler olarak hayal etme olasılıklarının kızlardan çok daha yüksek olduğunu ortaya koymaktadır. (Microsoft, 2017).

İstihdamda BİT uzmanları arasında kadınların payına bakıldığında, 2020'de AB27'de tüm BİT uzmanlarının yalnızca %18,5'i kadındı. Kadınların en büyük payı %28,2 ile Bulgaristan, %26,6 ile Yunanistan ve %26,2 ile Romanya'da gerçekleşti (bkz. grafik 5 (Women go tech, 2021)). İskandinav-Baltık bölgesinden gelen ülkeler de, ülke sıralamasının daha ortasında yer alan Norveç dışında, çoğunlukla listenin en üst sıralarında yer aldı. (Kadınlar teknolojiye gidiyor, 2021).

Litvanya Cumhuriyeti İstatistik Dairesi'ne göre, 2022'nin dördüncü çeyreğinde bilgi ve iletişim kategorisindeki çalışan sayısı 29,4 bin erkek ve 21,5 bin kadın oldu. 2023'ün ilk çeyreğinde 34,6 bin erkek, 20,7 bin kadın oldu. 2023'ün ikinci çeyreğinde 36,8 bin erkek ve 14,8 bin kadın, 2023'ün üçüncü çeyreğinde ise 34,5 bin erkek ve 18,0 bin kadın oldu. 2023'ün 1. çeyreğinden 2. çeyreğine kadar kadın çalışan sayısında gözle görülür bir düşüş ve ardından 2023'ün 3. çeyreğinde bir artış var (Rodiklių Duomenų Bazė - Oficialiosios Statistikos Portalas, t.y.).

Kadınların %11'inin siber güvenlik alanında çalıştığı bir ankette, kadınların bu alandaki bakış açılarına ilişkin kamuoyunun görüşlerini öğrenmek için bir anket yapıldı. Uyuşmazlıklarda katılımcıların %44,4'ü siber güvenlik alanındaki kadın sayısının %30 ile %60 arasında olması gerektiği yanıtını verdi. Ankete katılanların en büyük payı, kadınların kadın profesyonellerin %30 ila %60'ını (%35,2) oluşturması gerektiğini söyledi. Cinsiyet ve yaş grubuna göre yanıtlar incelendiğinde, kadınların, özellikle de gençlerin (25 yaş altı ve 25-45 yaş altı) en çok kadın sayısının yarı yarıya olması gerektiğini düşündükleri görülmektedir. Genç erkekler (25 yaş altı) kadınların %30'unun kadın olması gerektiğini düşünüyor. Kadınların kendilerinin Siber Güvenlik alanında şu anda piyasada olduğundan çok daha fazla sayıda kadın görme eğiliminde oldukları görülebilir. Bu iyi bir haber, çünkü kadınları sahaya çekmek sadece profesyonel eksikliğini gidermeye yardımcı olmakla kalmayacak, aynı zamanda kuruluşların güvenliğini de artıracaktır. (Bukauskas ve diğerleri, 2022).

Birçok Avrupa ülkesinde olduğu gibi Finlandiya'da da genel olarak siber güvenlik ve bilişim alanında cinsiyet dengesizliği konusunda ortak bir anlayış var. Kadınları siber güvenlik alanında desteklemeye ve siber güvenlik zorluklarının ele alınmasına katılımlarını teşvik etmeye yönelik girişimler ve çabalar arttı. Çoğu kar amacı gütmeyen kuruluşlar tarafından desteklenmektedir.

Siber güvenlik alanı, eğitim ve kariyer yolları, eğitim programları ve ağ oluşturma etkinlikleri geliştirmek için çeşitli girişimler gördü. Strateji aynı zamanda siber güvenlik alanında başarılı

kadın kariyer yolunu vurgulayarak rol modelleri teşvik etmeye ve daha fazla kadına bu alanda kariyer yapmaları için ilham vermek için hikayelerini paylaşmaya dayanıyor. Women4Cyber ve listelenen girişimler, yalnızca cinsiyet eşitsizliği dengesizliğini ele almak için değil, aynı zamanda siber güvenlik sektörünün genel gücüne ve dayanıklılığına katkıda bulunmak için çeşitlilik ve kapsayıcılığın önemini vurguluyor. Kamu ve özel kurumlar da tüm girişimlerinde bu toplumsal cinsiyet eşitliği boyutunu birinci öncelik olarak dahil ederek bu stratejiyi desteklemektedir.

Women4Cyber Finlandiya (W4CFI)

Ağustos 2021'de kurulan W4CFI, Finlandiya siber güvenlik sektöründe istihdam edilen kadın sayısını artırmayı amaçlayan kar amacı gütmeyen bir kuruluştur. AB çapındaki daha büyük Women4Cyber girişiminin bir parçasıdır ve Finlandiya'da daha çeşitli ve kapsayıcı bir endüstriyi desteklemeye odaklanmaktadır. W4CFI, kadınların siber güvenliğe katılımını artırmak ve desteklemek için rehberlik sağlamak, bilgi alışverişinde bulunmak ve farkındalık yaratmak da dahil olmak üzere çeşitli faaliyetlerde yer almaktadır. **Women4Cyber Finlandiya**

Finlandiya Ulaştırma ve Haberleşme Bakanlığı ve Aalto Üniversitesi Projesi

Finlandiya Ulaştırma ve Haberleşme Bakanlığı, Aalto Üniversitesi ile işbirliği içinde, siber güvenliği Avrupa Birliği genelinde bir yurttaşlık becerisi haline getirmek için bir eğitim paketi geliştiriyor. Bu girişim, siber güvenliğin günlük yaşamda artan önemini ve kadınlar da dahil olmak üzere tüm vatandaşlar arasında farkındalık ve beceri ihtiyacını vurgulamaktadır. Eğitim kurumlarının, bu alanda kadınları güçlendirmek için çok önemli olan erişilebilir siber güvenlik eğitimi ve öğretimi sağlamadaki rolünün altını çiziyor. Finlandiya, AB'de siber güvenlik becerileri eğitimini artırıyor. **Dijital Beceriler ve İşler Platformu** (europa.eu)

"Mimmit koodaa" (Kadın Kodu) hareketi

Bu girişim atölye çalışmaları, eğitim, ağ oluşturma fırsatları, web seminerleri ve kariyer desteği sunar. Klişelere meydan okumaya ve daha fazla kadını siber güvenlik de dahil olmak üzere teknoloji alanındaki kariyerleri keşfetmeye teşvik etmeye odaklanıyor. Bu kuruluş, kadınların siber güvenlik alanına girmeleri ve başarılı olmaları için yollar yaratmayı amaçlıyor. **Mimmit koodaa**

Agoria tarafından 2022'de yayınlanan Belçika'daki siber güvenlik sektörüyle ilgili ilk sosyo-ekonomik araştırmaya göre, Belçika siber güvenlik ortamında kadınlar işgücünün %19'unu temsil ediyor. Belçika Ekonomi Bakanlığı'nın (FPS Belçika) koordinasyonuyla, Belçika'daki yetkin politika oyuncuları, "Dijitalde Kadınlar – Ulusal ve Kesişimsel Strateji 2021-2026" adlı dijitalde kadınlar için beş yıllık bir plan hazırladı. Beş yıllık plan, önyargılarla mücadele etmek ve kadınların dijital ekonomiye katılımını engelleyen yapısal engellerin üstesinden gelmek için yararlı olan beş stratejik hedefe dayanan ortak ve sektörler arası bir strateji içeriyor. Beş hedef şunlardır:

1. Dijital sektörde daha fazla kadının mezun olmasını sağlamak; 2. Tüm kadınların dijital işgücü piyasasına ve/veya dijital sektöre katılımının teşvik edilmesi; 3. Kadınların dijital sektörde elde tutulmasını iyileştirmek; 4. Kadınların sahadaki rolünü (ekranda ve ekran dışında) tanıtmak için

yeni imajlar oluşturmak; 5. Belirli hedef gruplar arasındaki cinsiyet farkını kapatmak (**Stratejiye bağlantı**).

Merkezi Brüksel'de bulunan Women4Cyber Vakfı, Belçika ve Avrupa'da siber güvenlik alanında çalışan veya kariyerlerine yeni başlayan kadınları hedefleyen çok çeşitli etkinlikler düzenliyor ve destekliyor. Belçika'da Vakıf, bu faaliyetlerde Belçika Ulusal Bölümü'nü (**Women4Cyber Belgium**) desteklemekte ve işbirliği yapmaktadır. Belçika Ulusal Bölümü, girişimler üzerinde çalışan yaklaşık 20 aktif üyeye sahiptir. Bölüm tarafından düzenlenen faaliyetler, etkinlikler ve programlar şunlardır: W4C Belçika Bölümü'nün siber ve bilgi güvenliği ile ilgili çeşitli alanlardaki uzmanları konuşmaya davet ettiği "sanal kahve" gibi ağ oluşturma toplantıları ve etkinlikleri (sanal ve yüz yüze); web seminerleri ve bilgilendirme oturumları; kadınların becerilerini geliştirmelerine ve siber güvenlik kariyerlerini her düzeyde ilerletmelerine yardımcı olmayı amaçlayan mentorluk programları; Belçika Siber Güvenlik Koalisyonu ile işbirliği içinde projeler ve etkinlikler (**2023 Dünya Kadınlar Günü organizasyonu gibi**); Solvay Brussels School of Economics & Management tarafından düzenlenenler gibi siber ile ilgili eğitim programları için bursların teşvik edilmesi.

Norveç'te, siber güvenlikte cinsiyet farkını ele almak, esnek ve çeşitliliğe sahip bir iş gücü oluşturmak için çok önemlidir. BT'deki kadınların oranı sadece %29'dur. Düşük sayı, ortaöğretim düzeyinde matematik ve teknik konuları seçen kadınların sayısıyla büyük ölçüde bağlantılıdır.

Kadınları dahil etmek için eğitim ve destek ihtiyaçları ve tavsiyeleri

Kadınların katılımını teşvik etmek için özel olarak tasarlanmış özel siber güvenlik programlarına ihtiyaç var. Bu programlar, teknik yönleri kurumsal ve insan merkezli siber güvenlik konularıyla dengelemelidir. Alanda birkaç teknik ileri eğitim varken, çoğu tipik kadın mesleğinde (pedagojik – sağlık meslekleri) ileri eğitim teklifleri böyle bir teklife sahip değildir ve bu mesleklerle ilgili siber güvenlik konusunda daha kısa eğitim teklifleri geliştirmek daha fazla kadına ulaşabilir. Bu aynı zamanda, çeşitliliğin siber güvenlik zorluklarına benzersiz bakış açıları getirebileceğini belirten sektörün kendisi tarafından da destekleniyor. Okullarda ve üniversitelerde atölye çalışmaları, seminerler ve hedefli sosyal yardım programları aracılığıyla kadınlar arasında şirket içi siber güvenlik kariyerleri hakkında farkındalığın artırılması, daha fazla kadına bu alana girmeleri için ilham verebilir.

2022'de aday gösterilen en iyi 50 Norveçli kadın teknoloji kadınının birçoğu tarafından önerilen bir başka yaklaşım da, siber güvenlik alanındaki kadınlara temel rehberlik ve destek sağlamak, bu alanda gezinmelerine ve ilerlemelerine yardımcı olmak için mentorluk programları ve ağ oluşturma fırsatları oluşturmaktır.

Siber güvenlik sektörünün kendisi, kuruluşların kadınların siber güvenlik rollerinde işe alınmasını ve elde tutulmasını aktif olarak teşvik eden kapsayıcı işe alım uygulamaları ve politikaları uygulaması gerektiğini öne sürüyor. McKinsey'in «İşyerinde Kadınlar 2022 raporuna göre, teknik rollerdeki kadınların %32'si genellikle iş yerinde "odadaki tek kadın".

Son olarak, kadınları siber güvenlikte liderlik pozisyonlarına terfi ettirmek, rol modelleri sağlayabilir ve Mia Landsem gibi diğer kadınlara da benzer yolları izlemeleri için ilham

verebilirhttps://www.orangecyberdefense.com/no/innsikt/nyheter/mia-landsem-etisk-hacker-i-orange-cyberdefense-er-blant-norges-fremste-tech-kvinner.

Romanya'da siber güvenlik, en dinamik ve heyecan verici teknoloji sektörlerinden biri olmaya devam ediyor. Ancak bu sektörün kadınların temsili ve ücretlendirmesinde sistemik bir değişime ihtiyacı var. Siber güvenlik alanına olan ilginin artmasına rağmen, cinsiyet eşitsizliği devam ediyor. Kadınlar hala ciddi şekilde yetersiz temsil edilirken, çoğu iş ağırlıklı olarak erkektir. Siber güvenliğin geleceği, daha fazla kadın da dahil olmak üzere daha fazla siber profesyoneli çekme, elde tutma ve terfi ettirme yeteneğinden etkilenir.

Dünyada kadınların ne kadar az değerlendirildiğini göstermek, aynı zamanda kadınların her alanda, özellikle de siber güvenlikteki önemini herkesin anlamasını sağlamak için birçok çalışma yapıldı. Siber güvenlik çalışan tabanı arasındaki aşırı cinsiyet farkı, işteki diğer güçlerin hiç de eşit olmadığını gösteriyor. Kadınlar toplam işgücünün %39'unu oluşturuyor. Cybersecurity Ventures'a göre, STEM işlerinde çalışanların %38'ini, ancak siber güvenlik işgücünün yalnızca yaklaşık %25'ini oluşturuyorlar.

Kadınları siber güvenliğin dışında tutan çeşitli engeller var. Siber güvenlik eğitimi ve sertifikasyonuna odaklanan kar amacı gütmeyen bir kuruluş olan (ISC)2'nin araştırmasına göre, sahada çalışan kadınların çoğunluğu cinsiyete dayalı ayrımcılık bildiriyor. Kadınların neredeyse tamamı (%87) bilinçsiz ayrımcılığa maruz kaldıklarını bildirirken, %19'u açık ayrımcılığa maruz kaldıklarını söyledi. Kadınlar ayrıca kariyer gelişiminde açıklanamayan gecikmeler (% 53) ve hatalara abartılı tepkiler (% 29) gösterdiler.

Ayrımcılık aynı zamanda bir tazminat açığında da kendini gösterir. (ISC)2 araştırması, siber güvenlik alanında çalışan erkeklerin %32'sinin yılda ortalama 50.000 ila 100.000 dolar kazandığını, siber güvenlik alanındaki kadınların ise yalnızca %18'inin aynı gelir grubunda olduğunu gösteriyor. Ve erkeklerin %25'ine karşı kadınların %20'si yılda 100,000 ila 500,000 dolar kazanıyor.

Siber güvenlik alanında kadın sayısını artırmak için çeşitlilik, yenilikçilik, duygusal empati ve tarafsız bir bakış açısının faydaları gibi siber güvenlik alanında kadın sayısını artırmak için güçlü argümanlar var ve bunların tümü siber güvenlik işyeri için değerli becerilerdir.

Women in Cybersecurity yönetim kurulu üyesi Jay Koehler başka bir içgörü daha sağladı: "Kadınlar okulu bırakıyor çünkü burası bir 'erkek kulübü' ve düşük bir aidiyet duygusu var." Bu konu, psikolojik güvenlik ve toplumsal cinsiyet dostu bir işyeri sağlama taahhüdü ve hesap verebilirliği ve kadın ağları oluşturarak ele alınabilir.

Siber güvenliğin artık "erkek egemen bir meslek" değil, her cinsiyetten ve geçmişten yetenekli insanlarla dolu olacağına dair umut var.

İspanya'da kadınların siber güvenliğe katılımı ile ilgili literatür azdır. Mevcut literatürün çoğu, STEM disiplinleri de dahil olmak üzere daha geniş bilimsel toplulukta belirgin bir cinsiyet dengesizliği olduğunu ve kadınların daha yüksek kariyer aşamalarına ilerlemesinde gözle görülür bir azalma olduğunu göstermektedir ve bu genellikle bir "boru hattı fenomeni" olarak

kabul edilmektedir. Yüksek öğrenim açısından, cinsiyet farkı hala belirgindir ve bu konularda çalışmalarını tamamlayanların sadece %18'i kadındır. KOBİ'ler tarafından I+D ile ilgili pozisyonlar için istihdam edilen kadınlar hala çok düşük, Ulusal İstatistik Enstitüsü'nün verilerine göre %30'a bile ulaşmıyor. İspanya'daki yükseköğretim kurumları için siber güvenlik alanındaki kadın araştırmacılar açısından, çok azı cinsiyet açısından dengeli bir kadro sergilemektedir. *Fundación Alternativas tarafından incelenen 31 yükseköğretim kurumundan* 11'inde araştırma ekiplerinde hiç kadın yer almıyor ve bunlardan sadece 5'i daha eşitlikçi bir işgücü sergiliyor. Bu zorluklara yanıt olarak, eğitim ve destek ihtiyaç analizi, iyileştirilmesi gereken kilit alanları belirler. Daha fazla kadını doktora eğitimine devam etmeye teşvik etmek ve eğitim hattı boyunca dengeli bir temsil sağlamak için girişimler geliştirilmelidir. Kariyer geliştirme süreçlerindeki önyargıları ele almak çok önemlidir ve mentorluk programları, siber güvenlik alanının inceliklerinde kadınlara rehberlik etmede çok önemli bir rol oynayabilir. Ayrıca, kariyer yörüngelerini araştırmak ve kadınların özel sektörlerdeki siber güvenlik rollerine katılımını teşvik etmek için özel sektör kuruluşlarıyla işbirliği yapılması önerilmektedir. Niteliklerin ve yetkinliklerin değerlendirilmesi, belirli siber güvenlik becerilerini ve yetkinliklerini vurgulayarak özelleştirilmiş eğitim programlarının önemini vurgulamaktadır.

2.3. ESCO MESLEKLERININ ANALIZI

Bilgi, beceri ve yeterlilikler dahil olmak üzere belirlenen öğrenme çıktıları ile ilgili olarak mevcut ESCO (Avrupa çok dilli Beceri, Yeterlilikler ve Meslekler Sınıflandırması) sınıflandırmasını yorumluyoruz. Amaç:

- Siber güvenlikle ilgili mevcut ESCO mesleklerini analiz edin.
- Belirlenen öğrenme çıktılarını bilgi, beceri, yeterlilikler vb. açısından ESCO meslekleriyle eşleştirin.

Her meslek için bir dizi yeterlilik, beceri ve bilgi vardır. Aşağıda yeterlilik, beceri, bilgi ve değer tanımları ve örnekleri listelenmiştir.

Yetkinlik , bir bireyin belirli bir görevi veya işi etkili bir şekilde yerine getirme yeteneğini ifade eder. Performansı artırmak için uygulanan bilgi, beceri ve davranışların bir kombinasyonunu kapsar. Örnek: Proje yönetiminde yetkin olmak, organizasyon becerilerinin, proje yönetimi süreçleri bilgisinin ve ekip üyeleriyle etkili iletişim kurma becerisinin bir kombinasyonunu içerir.

Beceriler , bir bireyin görevleri yerine getirmesini sağlayan uygulama, eğitim veya deneyim yoluyla edinilen belirli yetenekler veya yeteneklerdir. Örnek: Sızma testi becerileri, siber güvenlik araçlarını ve yazılımlarını kullanma becerisi, programlama becerileri ve tehditleri gerçek zamanlı olarak analiz etme ve bunlara yanıt verme yeteneği.

Bilgi , eğitim veya deneyim yoluyla öğrenilen gerçekleri, bilgileri ve anlayışı ifade eder. Belirli bir alanla ilgili gerçeklerin ve ilkelerin teorik anlayışını kapsar. Örnek: Farklı siber saldırı türlerinin (örneğin, kimlik avı, fidye yazılımı, DDoS saldırıları) nasıl gerçekleştirildiğini anlamak veya çeşitli

şifreleme yöntemleri hakkında bilgi sahibi olmak ve siber güvenlikteki en son trendlere ve gelişmelere aşina olmak.

Bu analiz 2 aşamaya ayrılmıştır:

Aşama 1: ESCO Mesleklerinin gözden geçirilmesi ve seçimi

Siber güvenlikle ilgili meslekleri filtrelemek ve bir sonraki bölümde her mesleği belgelemek, listelenen becerilere, yetkinliklere, bilgilere özel dikkat göstermek için ESCO portalında danışmanlık.

ESCO Meslek Unvanı	Bilgi	Beceri	Yetkinlik
3512.3 - BİT güvenlik teknisyeni	• BİT ağı • Donanım Saldırı Vektörleri • Siber saldırılara karşı önlemler • BİT'in işletim sistemleri tedariki • Ağ Ekipmanları • Web uygulaması • Güvenlik tehditleri	• Sorunları eleştirel bir şekilde ele alın • BİT sistemini analiz etmek • Uygun belge yönetimini sağlayın • yazılım testleri yürütmek, BİT sistemi zayıflıklarını belirlemek	• Sistem bileşenlerini entegre edin • Teknik dokümantasyon sağlayın • BİT sistemi sorunlarını çözmek • Erişim kontrol yazılımı kullanın
2529.1 - Baş BİT Güvenlik Görevlisi - Kurumsal güvenlik işlevlerini yerine getiren kişileri içerir.	• BİT ağ güvenliği riskleri • BİT güvenlik mevzuatı • BİT güvenlik standartları • Saldırı vektörleri • Denetim teknikleri • Siber saldırılara karşı önlemler • Siber Güvenlik • Veri koruma • Karar Destek Sistemleri • Bilgi Gizliliği • Bilgi Güvenliği Stratejisi • İç Risk Yönetimi Politikası • Organizasyonel dayanıklılık	• Veri gizliliği konusunda eğitin • Kurumsal BİT standartlarına uyulmasını sağlamak • Yasal gerekliliklere uygunluğu sağlayın • Departmanlar arası işbirliğini sağlayın • Bilgi gizliliğini sağlayın • BİT güvenlik risklerini belirleyin • BİT risk yönetimini uygulamak • BİT güvenlik politikalarını uygulamak • Kurumsal Yönetişimi Uygulayın	• Olağanüstü durum kurtarma tatbikatlarına liderlik edin • Operasyonların sürekliliği için plan yapın • BT güvenlik uyumluluklarını yönetin • Felaket kurtarma planlarını yönetin • Uzmanlık alanındaki gelişmeleri izlemek • Teknoloji trendlerini izleyin Karar Destek Sisteminden Faydalanmak
2529.2 - Adli Bilişim Uzmanı - Bilgisayarlardan ve diğer veri depolama aygıtlarından bilgi alır ve analiz eder; gizlenmiş, şifrelenmiş veya zarar görmüş olabilecek dijital medyayı, dijital bilgileri tanımlamak, korumak, kurtarmak, analiz etmek ve bunlarla ilgili gerçekleri ve	• BİT ağ güvenliği riskleri • BİT güvenlik standartları • Adli Bilişim • Siber saldırılara karşı önlemler • Bilgi Gizliliği • Sızma Testi Aracı • Sorgu dilleri	• Tersine mühendislik uygulayın • Bilgi güvenliği stratejisi geliştirin • Veri gizliliği konusunda eğitin • Adli amaçlar için veri toplayın • BİT güvenlik risklerini	• BT güvenlik uyumluluklarını yönetin • Yasal konular için verileri yönetin • Dijital cihazların adli korumalarını gerçekleştirin

görüşleri sunmak amacıyla adli bir şekilde inceler.	• Kaynak Açıklama Çerçevesi Sorgu Dili	belirleyin • BİT sisteminin zayıflıklarını belirleyin • ICT ağ tanılama araçlarını uygulayın • BİT danışmanlığı tavsiyesi sağlamak • Hassas müşteri bilgilerinin güvenliğini sağlayın • Komut dosyası programlamayı kullanma • Veri koruma için yazılım kullanın • BİT güvenlik testi yapmak	
2529.3 - Gömülü Sistemler Güvenlik Mühendisi - Gömülü Sistem Güvenlik Mühendislerinin odak noktası, bağlantılı ürünler ve bunların destekleyici ağlarıdır ve BİT güvenlik mühendisinde olduğu gibi kurumsal güvenlikten daha azdır.	• BİT ağ güvenliği riskleri • BİT güvenlik standartları • Nesnelerin İnterneti • Bilgisayar Programcılığı • Siber saldırılara karşı önlemler • Gömülü Sistemler • Bilgi Güvenliği Stratejisi • Yazılım anormallikleri	• BİT sistemini analiz etmek • Akış Şeması Diyagramı Oluştur • Güvenlik ilkelerini tanımlayın • ICT aygıt sürücüsü geliştirin • Yazılım prototipi geliştirin • Yazılım testlerini yürütün • BİT güvenlik risklerini belirleyin • BİT sisteminin zayıflıklarını belirleyin • Teknik metinleri yorumlayabilme • BİT danışmanlığı tavsiyesi sağlamak • BİT güvenlik testi yapmak • Teknik dokümantasyon sağlayın	• En son bilgi sistemleri çözümlerini takip edin • BT güvenlik uyumluluklarını yönetin • Sistem performansını izleme • Risk analizi yapmak • Rapor testi bulguları yazılım tasarım desenlerini kullanır • Yazılım kitaplıklarını kullanın • Bilgisayar destekli yazılım mühendisliği araçlarını kullanmak • Teknik gereksinimleri tanımlayın
2529.4 - Etik Hacker - Endüstride kabul görmüş yöntem ve protokollere uygun olarak güvenlik açığı değerlendirmeleri ve sızma testleri gerçekleştirir; Yanlış sistem yapılandırmasından, donanım veya yazılım kusurlarından veya operasyonel zayıflıklardan kaynaklanabilecek olası güvenlik açıkları için	• Saldırı vektörleri • Adli Bilişim • Siber saldırılara karşı önlemler • etik • BİT ürünlerinin yasal gereklilikleri • Sızma Testi Aracı • Yazılım anormallikleri • BİT test otomasyonu için araçlar	• BİT güvenlik testi yapmak • Teknik dokümantasyon sağlayın • Kod açıklarından yararlanma geliştirin • BİT denetimlerini yürütmek • Yazılım testlerini yürütün	• Sorunları eleştirel bir şekilde ele alın • Bir kuruluşun bağlamını analiz edin • Sistem performansını izleme

sistemleri analiz eder.	• Web uygulaması güvenlik tehditleri	• BİT güvenlik risklerini belirleyin • BİT sisteminin zayıflıklarını belirleyin	
2529.5 - BİT dayanıklılık yöneticisi - bir kuruluşun siber güvenliğini, dayanıklılığını ve felaket kurtarmayı geliştiren modelleri, politikaları, yöntemleri, teknikleri ve araçları araştırır, planlar ve geliştirir	• BİT kurtarma teknikleri • Siber Güvenlik İç • Risk Yönetimi Politikası • Organizasyonel dayanıklılık • Sistem Yedekleme En İyi Uygulaması	• Acil durumlar için acil durum planları geliştirmek • Bilgi güvenliği stratejisi geliştirin • BİT denetimlerini yürütmek • BİT güvenlik risklerini belirleyin • BİT kurtarma sistemini uygulamak • BİT risk yönetimini uygulamak	• İş süreçlerini analiz edin • Bir kuruluşun bağlamını analiz edin • Yasal mevzuatlara uymak • Olağanüstü durum kurtarma tatbikatlarına liderlik edin • BT güvenlik uyumluluklarını yönetin • Felaket kurtarma planlarını yönetin • Sistem güvenliğini yönetin • BİT güvenlik testi yapmak
2529.6 - BİT güvenlik yöneticisi - bilgi ve verileri yetkisiz erişime, kasıtlı saldırıya, hırsızlığa ve yolsuzluğa karşı korumak için güvenlik önlemleri planlar ve uygular.	• BİT ağ güvenliği riskleri • Nesnelerin İnterneti • Siber saldırılara karşı önlemler • Veritabanı Geliştirme Araçları • İnternet Yönetişimi • Mobil Cihaz Yönetimi • İşletim sistemleri • Organizasyonel dayanıklılık • Kalite güvence metodolojileri • Sistem Yedekleme En İyi Uygulaması	• BİT sisteminin zayıflıklarını belirleyin • Teknik metinleri yorumlayabilme • BİT kimlik yönetimini sürdürmek • Veritabanı güvenliğini koruyun	• Şirket politikalarını uygulayın • BİT sistemlerinin kalitesine katılmak • Uygun belge yönetimini sağlayın • ICT veri mimarisini yönetin • BT güvenlik uyumluluklarını yönetin • BİT sorun giderme gerçekleştirme • BİT sistemi sorunlarını çözmek
2529.7 - BİT güvenlik mühendisi - verilere ve programlara erişimi kontrol etmek için çözümler önerir ve uygular ve kuruluşun misyonunun ve iş süreçlerinin korunmasını sağlar.	• BİT güvenlik mevzuatı • BİT güvenlik standartları • Saldırı vektörleri • İş Analizi • Siber saldırılara karşı önlemler • Siber Güvenlik • Ortaya çıkan teknolojiler • Bilişim Mimarisi • Bilgi Güvenliği Stratejisi • İşletim sistemleri • Organizasyonel dayanıklılık • Risk Yönetimi • Yapılandırılmamış veriler	• Bilgi güvenliği stratejisi geliştirin • Veri gizliliği konusunda eğitin • Bilgi güvenliğini sağlayın • BİT denetimlerini yürütmek • Yazılım testlerini yürütün • BİT güvenlik risklerini belirleyin • BİT sisteminin zayıflıklarını belirleyin • BİT risk yönetimini uygulamak • BİT danışmanlığı	• Veri kalitesi kriterlerini tanımlayın • Teknik gereksinimleri tanımlayın • Görev kayıtlarını tutun • En son bilgi sistemleri çözümlerini takip edin • BT güvenlik uyumluluklarını yönetin • Felaket kurtarma planlarını yönetin • Sistem performansını izleme • Veri analizi gerçekleştirin • Risk analizi yapmak • Test bulgularını bildirme sorun giderme

		tavsiyesi sağlamak • BİT sistemini analiz etmek • Güvenlik ilkelerini tanımlayın	• resmi ICT spesifikasyonlarını doğrulayın
2529.8 - BİT güvenlik yöneticisi - gerekli güvenlik güncellemelerini önerir ve uygular; tavsiyelerde bulunur, destekler, bilgilendirir ve eğitim ve güvenlik bilinci sağlar ve bir ağın veya sistemin tamamı veya bir kısmı üzerinde doğrudan eylemde bulunur.	• BİT problem yönetimi teknikleri • BİT proje yönetimi • BİT kalite politikası • BİT güvenlik standartları • ICT sistemi kullanıcı gereksinimleri • Nesnelerin İnterneti • Saldırı vektörleri • Adli Bilişim • Bilgi Güvenliği Stratejisi • İç Risk Yönetimi Politikası • İnternet Yönetişimi • BİT ürünlerinin yasal gereklilikleri	• Güvenlik ilkelerini tanımlayın • Bilgi güvenliği stratejisi geliştirin • bir BİT güvenlik önleme planı oluşturmak • BİT risk yönetimini uygulamak	• Olağanüstü durum kurtarma tatbikatlarına liderlik edin • BİT kimlik yönetimini sürdürmek • BT güvenlik uyumluluklarını yönetin • Felaket kurtarma planlarını yönetin • BİT sistemi sorunlarını çözmek
2529.9 - Bilgi Mühendisi - Normalde yüksek düzeyde insan uzmanlığı veya yapay zeka yöntemleri gerektiren karmaşık sorunları çözmek için yapılandırılmış bilgiyi bilgisayar sistemlerine (bilgi tabanları) entegre eder.	• İş Zekası • İş Süreçleri Modelleme • Veritabanı Geliştirme Araçları • Bilgi çıkarma • Bilgi Yapısı Doğal Dil İşleme • Yapay Zekanın İlkeleri • Kaynak Açıklama Çerçevesi Sorgu Dili • Sistem geliştirme yaşam döngüsü • Sistem Teorisi • Görev algoritması • Web Programlama	• Uygulamaya özel bir arayüz kullanın • Veritabanlarını kullanma • İşaretleme dillerini kullanma	• İş gereksinimlerini analiz edin • BİT sistemleri teorisini uygulamak • BİT bilgisini değerlendirmek • Anlamsal ağaçlar oluşturma • Teknik gereksinimleri tanımlayın • BİT anlamsal entegrasyonunu yönetmek • İş Bilgisini Yönetin • Veritabanını Yönet

Aşama 2: ESCO Mesleğini ve öğrenme çıktılarını haritalama

Önceki tablo ile belgelenmiş meslekleri analiz ettik ve her bir rolle ilişkili öğrenme çıktılarını belirledik. Bu sonuçları bilgi, beceri ve yetkinlikler olarak kategorize etmek için ESCO çerçevesini kullandık.

Öğrenme çıktısı, öğrencilerin bir öğretim döneminin sonunda ne öğrenmeleri ve yapabilmeleri beklendiğini açıklayan açık ve spesifik bir ifadedir. İfade bilgi, beceri ve tutumları içerir.

ESCO meslekleri sınıflandırıcı bölümünde Bilgi ve iletişim teknolojisi uzmanları iki alt bölümde yer alır: Yazılım ve uygulama geliştiricileri ve analizi ve Veritabanı ve ağ uzmanları. Sonuncusu dört gruptan oluşur: Veritabanı ve ağ uzmanları, Sistem yöneticileri, Bilgisayar ağı uzmanları ve başka yerde sınıflandırılmamış veritabanı ve ağ uzmanları. Tabloda sunulan tüm siber güvenlik meslekleri bu birim grubunda bulunmuştur. Örneğin, grup bilgi ve iletişim teknolojisi güvenlik uzmanlarını içerir.

Bu gibi durumlarda, görevler şunları içerir:

(a) bilgisayar dosyalarını kazara veya yetkisiz olarak değiştirilmeye, imha edilmeye veya ifşa edilmeye karşı korumak ve acil durum veri işleme ihtiyaçlarını karşılamak için planlar geliştirmek.

(b) sistem güvenliğini sağlamak ve sunucu ve ağ verimliliğini artırmak için kullanıcıları eğitmek ve güvenlik bilincini teşvik etmek.

(c) bilgisayar verilerine erişim ihtiyaçları, güvenlik ihlalleri ve programlama değişiklikleri gibi konuları tartışmak için kullanıcılarla görüşmek.

(d) Virüs koruma sistemlerinin ne zaman güncelleneceğini belirlemek için mevcut bilgisayar virüsü raporlarını izlemek.

(e) yeni yazılım eklemek, hataları düzeltmek veya bireysel erişim durumunu değiştirmek için bilgisayar güvenlik dosyalarını değiştirmek.

(f) veri dosyalarının kullanımını izlemek ve bilgisayar dosyalarındaki bilgileri korumak için erişimi düzenlemek.

(g) Veri işleme faaliyetlerinin ve güvenlik önlemlerinin işleyişini sağlamak için risk değerlendirmeleri yapmak ve veri işleme sisteminin testlerini yürütmek.

(h) veri aktarımlarını şifrelemek ve gizli bilgileri iletilirken gizlemek ve kusurlu dijital aktarımları dışarıda tutmak için güvenlik duvarları oluşturmak.

Her meslek için öğrenme çıktılarının açıklaması:

Meslek	Dersin öğrenme çıktıları
BİT güvenlik teknisyeni (3512.3)	• BİT ağları, donanım saldırı vektörleri, siber saldırı önlemleri ve işletim sistemleri hakkında kapsamlı bir anlayış gösterin. • Sistem güvenliğini artırmak için ICT sistemlerindeki güvenlik açıklarını eleştirel olarak analiz edin ve teşhis edin. • ICT güvenlik protokollerine uyan sağlam belge yönetimi stratejileri uygulayın ve yönetin. • Yazılım güvenlik açıklarını belirlemek ve düzeltmek için ayrıntılı yazılım test planları geliştirin ve yürütün. • Güvenli ve verimli ICT sistemleri oluşturmak için sistem bileşenlerini entegre edin ve erişim kontrol yazılımı kullanın.
BİT Güvenlik Sorumlusu (2529.1)	• Kurumsal bilgileri korumak için BİT ağ güvenliği risklerini, mevzuatını ve standartlarını anlayın ve analiz edin. • Bilgi güvenliği stratejileri ve şirket içi risk yönetimi politikaları geliştirmek ve uygulamak. • Olağanüstü durum kurtarma tatbikatlarına liderlik edin ve operasyonel süreklilik planlarını

	sürdürün. • Personeli veri gizliliği konusunda eğitin ve gelişmiş güvenlik uygulamaları için depart-manlar arası işbirliği sağlayın.
Adli Bilişim Uzmanı (2529.2)	• Özellikle Nesnelerin İnterneti (IoT) ortamında gömülü sistemlerin güvenliğini analiz edin ve test edin. • Yazılım prototipleri ve testleri geliştirin ve yürütün ve bilgisayar destekli yazılım mühendisliği araçlarını kullanın. • BT güvenlik uyumluluklarını yönetin ve risk analizi ve sistem performansı izleme gerçekleştirin. • Gömülü sistemler için güvenlik politikalarını ve teknik gereksinimleri tanımlayın ve uygulayın.
Gömülü Sistemler Güvenlik Mühendisi (2529.3)	• Özellikle Nesnelerin İnterneti (IoT) ortamında gömülü sistemlerin güvenliğini analiz edin ve test edin. • Yazılım prototipleri ve testleri geliştirin ve yürütün ve bilgisayar destekli yazılım mühendisliği araçlarını kullanın. • BT güvenlik uyumluluklarını yönetin ve risk analizi ve sistem performansı izleme gerçekleştirin. • Gömülü sistemler için güvenlik politikalarını ve teknik gereksinimleri tanımlayın ve uygulayın.
Etik Hacker (2529.4)	• Sektörde kabul görmüş yöntemleri kullanarak güvenlik açığı değerlendirmeleri ve sızma testi gerçekleştirin. • Güvenlik önlemlerini iyileştirmek için sistem-lerdeki olası güvenlik açıklarını belirleyin ve bunlardan yararlanın. • Sistem bütünlüğünü sağlamak için kod açıkları geliştirin ve ICT denetimleri gerçekleştirin. • Güvenlik stratejilerini etkili bir şekilde uyarla-mak için bir kuruluşun bağlamını analiz edin
BİT Dayanıklılık Yöneticisi (2529.5)	• Acil durum senaryoları için acil durum planları ve bilgi güvenliği stratejileri geliştirin ve uygu-layın. • ICT kurtarma sistemlerini ve risk yönetimi sü-reçlerini uygulayın ve yönetin. • Felaket kurtarma tatbikatlarına liderlik edin ve krizler sırasında sistem güvenliğini yönetin. • Kurumsal dayanıklılığı ve yasal düzenlemelere uyumu artırmak için iş süreçlerini analiz edin.
ICT Güvenlik Yöneticisi (2529.6)	• Verileri korumak ve ICT kimlik sistemlerini yönetmek için güvenlik önlemleri planlayın ve

	uygulayın. • Veritabanı güvenliğini koruyun ve sistem bütünlüğünü ve esnekliğini sağlayın. • ICT sistem sorunlarını çözün ve sorun giderme ve kalite güvence metodolojileri gerçekleştirin. • Veri mimarisini yönetin ve veri koruması için kurumsal ilkelere bağlı kalın.
BİT Güvenlik Mühendisi (2529.7)	• Verilere erişimi kontrol etmek ve iş süreçlerini korumak için çözümler önerin ve uygulayın. • BİT sistemlerini analiz edin ve güvenlik politikalarını ve veri kalitesi kriterlerini tanımlayın. • Veri analizi ve risk analizi gerçekleştirin ve BT güvenlik uyumluluklarını ve felaket kurtarma planlarını yönetin. • Ortaya çıkan teknolojiler ve bilgi sistemleri çözümleri ile güncel kalın
BİT Güvenlik Yöneticisi (2529.8)	• Güvenlik güncellemelerini önerin ve uygulayın ve çeşitli projelerde BİT güvenliğini yönetin. • Felaket kurtarma tatbikatlarına liderlik edin ve BİT güvenlik önleme planları oluşturun. • ICT kimlik yönetim sistemlerini koruyun ve yönetin ve karmaşık sistem sorunlarını çözün. • Bilgi güvenliği stratejileri geliştirin, uygulayın ve felaket kurtarma planlarını yönetin.
Bilgi Mühendisi (2529.9)	• RDF sorgu dili ve web programlama gibi gelişmiş araçları kullanarak yapılandırılmış bilgileri bilgisayar sistemlerine entegre edin. • İş bilgisi yönetimini geliştirmek için anlamsal entegrasyon ve veritabanı sistemlerini yönetin. • İş gereksinimlerini analiz edin ve etkili bilgi tabanları geliştirmek için BİT sistemleri teorisini uygulayın. • Yapay zeka yöntemlerini kullanarak karmaşık sorunları çözmek için anlamsal ağaçlar oluşturun ve BİT bilgisini değerlendirin.

3. ANALIZ VE BULGULAR

3.1. SAHA ARAŞTIRMASININ ANALIZI

Mesleki Eğitim ve Öğretim saha araştırması analizi

"KOBİ Siber Güvenlik Değişim Ajanları için Eğitim İhtiyaçlarının Haritalanması" anket verileri, Mesleki Eğitim ve Öğretim (VET) ve Yüksek Öğretim Kurumları (HEI) bağlamında siber güvenlik eğitimine odaklanan bir dizi soru içermektedir. Siber güvenlik eğitiminde yer alan konular, öğretim yöntemleri, cinsiyet kapsayıcılığı ve katılımcıların demografik özellikleri hakkında veri topladık.

Bu çalışmanın amacı, siber güvenlik eğitiminin mevcut durumunu, kullanılan metodolojileri ve bu alandaki kapsayıcılık ve etkililiğe ilişkin algıları anlamak için verilen yanıtları analiz etmektir.

Yanıt analizi aşağıdaki temel yapıya dayanacaktır:

- Demografik
- Müfredat, eğitim ihtiyaçları ve öğrenme tercihleri
- Yetkinlik gereksinimleri ve gelecekteki beceriler
- Cinsiyete özel içgörüler

Demografik:

Ankete katılanlar arasında Mesleki Eğitim ve Öğretim (VET) kurumları ile Yüksek Öğretim Kurumları (HEI) arasındaki cinsiyet dağılımı aşağıdaki gibidir:

Kurum Türüne Göre Toplam Yanıtlayan Sayısı

Kurum türü	Yanıt	Dişi	Erkek	Söylememeyi tercih ederim
HEI (Yüksek Öğretim Kurumları)	104	28	73	3
VET (Mesleki Eğitim ve Öğretim)	86	36	48	2
Toplam	**190**	**64**	**121**	**5**

Hem yükseköğretim hem de mesleki eğitim kurumlarında cinsiyet dengesizliği varken, mesleki eğitim kurumlarında bu fark daha dardır. Her bir kurumdan gelen toplam yanıt sayısına göre cinsiyet temsilinin daha net bir resmini sağlamak ve yanıt yanlılığı sayısıyla ilgili sonuçları ayarlamak için, her bir kurum türündeki her bir cinsiyetin yüzdesini hesapladık.

Katılımcıların Kurum Türüne Göre Dağılımı

Kurum türü	Kadın %	Erkek %	% Söylememeyi tercih ederim	Toplam
HEI (Yüksek Öğretim Kurumları)	27	70	3	**100%**
VET (Mesleki Eğitim ve Öğretim)	42	56	2	**100%**

Yanıt yanlılığına göre düzeltilmiş analiz, her iki kurum türünün de daha yüksek bir erkek katılımcı oranına sahip olmasına rağmen, Mesleki Eğitim kurumlarında erkek ve kadın temsili arasındaki farkın daha küçük kaldığını doğrulamaktadır. Bunun nedeni çeşitli olabilir (örneğin, bu kurum türleri arasında siber güvenlik eğitiminde cinsiyet çeşitliliğini etkileyen kültürel, yapısal veya politika faktörleri). Mesleki Eğitim ve Öğretimdeki kadın katılımcıların daha yüksek yüzdesi, mesleki eğitimde yüksek öğrenime kıyasla daha toplumsal cinsiyeti daha kapsayıcı bir ortamı destekleyen uygulamalara ilişkin daha fazla araştırma yapılması için potansiyel alanlar olduğunu göstermektedir.

Müfredat, eğitim ihtiyaçları ve öğrenme tercihleri

HEI ve VET mevcut siber güvenlik eğitimlerinde yer alan konular

Konu	Yanıt	Yükseköğretim Kurumu (HEI)	MEÖ
Siber güvenlik temelleri	151	90	61
Ağ güvenliği	123	72	51
Tehdit analizi ve yönetimi	99	65	34
Şifreleme	92	57	35
Olay müdahalesi	82	49	33
Risk yönetimi	77	43	34
Siber güvenlik yasaları ve politikaları	73	42	31
Gelişmiş tehdit azaltma teknikleri	54	33	21

Temel bilgi ve becerilerin ve ağ güvenliğinin bir öncelik olduğu görülmektedir. Tehdit Analizi ve Yönetimi, Kriptografi ve Olay Müdahalesi, eğitimlerde siber güvenlik tehditlerinin kapsamlı bir şekilde ele alınmasını önermektedir. Risk Yönetimi ve Siber Güvenlik Yasaları ve Politikaları, yasal bağlamı anlamayı ve riskleri etkin bir şekilde yönetmeyi içeren bütüncül bir yaklaşıma duyulan ihtiyacın farkındalığına işaret etmesine rağmen her zaman seçilmemektedir. Gelişmiş tehdit azaltma tekniklerinin eğitimlere daha az dahil edildiğini belirtmek ilginçtir.

Sonuçları, her bir kurum türünden (HEI ve VET) yanıt verenlerin sayısının getirdiği önyargı olmadan sağlamak için, veriler her bir kurum türü için toplam yanıt sayısı ile normalleştirildi. Bu yaklaşım, siber güvenlik eğitim programlarında her bir konuya yer veren kurumların oranını görmemizi sağlıyor.

Konu	HEI Oranı	Mesleki Eğitim Oranı
Siber güvenlik temelleri	15.76%	15.48%
Ağ güvenliği	12.61%	12.94%
Tehdit analizi ve yönetimi	11.38%	8.63%
Şifreleme	9.98%	8.88%
Olay müdahalesi	8.58%	8.38%
Risk yönetimi	7.53%	8.63%
Siber güvenlik yasaları ve politikaları	7.36%	7.87%
Gelişmiş tehdit azaltma teknikleri	5.78%	5.33%

İlginç bir şekilde, küçük farklılıklarla benzer öncelikler var. Hem HEI hem de MET kurumları "Siber Güvenlik Temelleri" ve "Ağ Güvenliği" üzerine büyük önem vermektedir. Bu, bu konuların siber güvenlik eğitiminin kritik bileşenleri olarak kabul edildiğini gösterir. Oranlar, Mesleki Eğitim ve Öğretim kurumlarına kıyasla HEI'lerde biraz daha fazla vurgulanan "Siber Güvenlik Temelleri" ve benzer bir model gösteren ancak daha dar bir boşlukla "Ağ Güvenliği" ile yakından eşleşmektedir.

"Tehdit Analizi ve Yönetimi", "Kriptografi" ve "Gelişmiş tehdit azaltma teknikleri" gibi daha özel konulara yapılan vurguda gözle görülür bir farklılık vardır. Yükseköğretim kurumları, Mesleki Eğitim ve Öğretim programlarına kıyasla eğitim programlarının biraz daha yüksek bir oranını bu konulara ayırma eğilimindedir. Yükseköğretim kurumlarının, genellikle daha geniş bir uzmanlık alanı içeren daha kapsamlı, teoriye dayalı bir siber güvenlik anlayışı sağlamaya odaklanması gerçeğiyle açıklanabilir. Öte yandan, Mesleki Eğitim ve Öğretim kurumları, hala geniş bir konu yelpazesini kapsarken, pratik uygulamalara ve acil işe hazır olmaya öncelik verebilir.

Öğretim yöntemleri

Öğretim Yöntemleri	HEI Oranı	Mesleki Eğitim Oranı
Örnek olay incelemeleri	60.91%	39.09%
Grup projeleri	58.95%	41.05%
Uygulamalı laboratuvarlar	59.02%	40.98%
Ders	56.97%	43.03%
Ters yüz sınıf	34.78%	65.22%
Çevrimiçi simülasyonlar	51.35%	48.65%

Vaka Çalışmaları, Grup Projeleri, Uygulamalı Laboratuvarlar, Ders Anlatımı yöntemleri, her iki kurum türünde de yaygın olarak kullanılmaktadır ve Mesleki Eğitim ve Öğretimden ziyade HEI'de tercih edilmektedir. Ters yüz sınıf yöntemi ile ilgili olarak, mesleki eğitimde (%65.22) yükseköğretim kurumuna (%34.78) göre daha yaygındır ve bu da mesleki eğitimde etkileşimli öğrenme modeline yönelik bir eğilimi göstermektedir. Ters yüz sınıflar, Mesleki Eğitim ve Öğretimin uygulamalı ve beceriye dayalı yaklaşım özelliğiyle iyi uyum sağlayan aktif öğrenmeye ve öğrenci katılımına öncelik verir.

Öğretim yöntemlerinin etkililiği

Öğretim Yöntemi	Sayı
Uygulamalı uygulama oturumları	141
Yüz yüze atölye çalışmaları	134
Etkileşimli animasyonlar	104
Çevrimiçi kurslar	100
Video eğitimleri	73
İnternet Seminerleri	68

Bu genel bakış, tercih edilen öğretim yöntemlerindeki çeşitliliği vurgular, ancak pratik, etkileşimli ve esnek öğrenme deneyimlerine açık bir vurgu yapar. Uygulamalı uygulama oturumları ve yüz yüze atölye çalışmaları, etkileşimli ve pratik bir öğrenme deneyimi sağladıkları

için çok değerlidir. Etkileşimli simülasyonlar ve çevrimiçi kurslar da erişilebilir öğrenme yöntemlerinin önemini gösteren önemli sözler aldı.

Okul kurumlarının karşılaştığı zorluklar.

Okul kurumlarının karşılaştığı temel zorluklar sorulduğunda, en çok tekrarlanan konuların bir özeti:

- **Katılımcı Beceri ve Deneyimlerinin Çeşitliliği**: Eğitmenler, katılımcılar arasındaki farklı geçmişler ve uzmanlık seviyeleri nedeniyle zorluklarla karşılaşmaktadır. Eğitimi tüm gruba uyacak şekilde uyarlamak ve hem teknik hem de teknik olmayan bireylerin oturumlardan yararlanabilmesini sağlamak zordur.
- **Kurs Materyalini Güncel** Tutmak: Siber güvenlik tehditlerinin hızlı evrimi, alaka düzeyini sağlamak için eğitim materyallerinde ve öğretim yöntemlerinde sürekli güncellemeler gerektirir.
- **Pratik Eğitim Kısıtlamaları**: Uygulamalı deneyim sağlamada önemli bir zorluk vardır. Sınırlamalar arasında yetersiz laboratuvar tesisleri, gerçek dünya simülasyon yeteneklerinin eksikliği ve uygulama için gerçekçi siber saldırı senaryoları oluşturmanın zorluğu yer alır.
- **Kaynak Sınırlamaları**: Eğitmenler genellikle sınırlı mali kaynaklar, kalifiye personel eksikliği, güncel olmayan çalışma materyalleri ve etkili eğitim için gerekli donanım ve yazılım araçlarının yetersizliği ile uğraşmak zorunda kalırlar.
- **Öğrenci Katılımı ve Motivasyonu**: Öğrencilerin dikkatini çekmek ve öğrenimlerine aktif olarak katılmaları için onları motive etmek, özellikle karmaşık ve bazen kuru teknik içeriği ele alma ihtiyacı nedeniyle zordur.
- **Müfredat ve Eğitim Yapısı**: Siber güvenliğin tüm yönlerini kapsayan kapsamlı, çok disiplinli müfredata ihtiyaç vardır. Ayrıca, siber güvenliği, özellikle lise düzeyinde, müfredata dahil etmek önemli bir zorluk olmaya devam ediyor.
- **Güncel Araç ve Teknolojilere Erişim**: Öğrencilere uygulamalı öğrenme için en son siber güvenlik araçlarına ve teknolojilerine erişim sağlamak genellikle zordur ve bu da pratik anlayış için çok önemlidir.
- **Dil ve Yerelleştirme Sorunları**: Siber güvenlik kaynakları her zaman öğrencilerin ana dillerinde bulunmayabilir ve bu da İngilizce konuşulmayan bölgelerdeki eğitime bir karmaşıklık katmanı ekler.
- **Endüstri ve Eğitim Uyumu**: Teorik temelleri öğretme ihtiyacını, endüstrinin ihtiyaçlarına uygun pratik becerilerle dengelemek zor bir iştir. Öğrencileri ilgili becerilerle iş piyasasına hazırlamak için de bir gereklilik vardır.
- **Öğretmen Kapasitesi ve Gelişimi**: Eğitimcilerin güncel bilgilere sahip olmalarını ve karmaşık kavramları etkili bir şekilde aktarabilmelerini sağlamak çok önemli ancak zordur.

KOBİ'lerin özel ihtiyaçlarına uyum

Yanıt Seçeneği	Sayı
Nötr	82
Hiza -lanmış	67
Biraz hizalanmamış	19
Son derece hizalı	17
Hizalanmamış	5

Yanıtların çoğu, bu noktada iyileştirme için yer olduğunu düşündüren nötr bir hizalamaya işaret ediyor. Ankete katılanların önemli bir kısmı programlarını uyumlu olarak değerlendirirken, çok az sayıda eğitimci programlarının son derece uyumlu olduğuna veya endüstri ihtiyaçlarıyla

uyumlu olmadığına inanıyor. Ölçeğin alt ucundaki yanıtlar (Hizalanmamış ve biraz hizalanmamış), eğitim içeriğini sektördeki siber güvenliğin gelişen doğasıyla tam olarak uyumlu hale getirme konusundaki endişeleri veya zorlukları yansıtıyor. Yanıtların bu dağılımı, endüstri trendlerine ve gereksinimlerine uyarlanmış siber güvenlik eğitimi sağlama zorluğunun hala geçerli olduğunu göstermektedir. Siber güvenlik eğitim programlarının siber güvenlik endüstrisinin ihtiyaçlarıyla uyumunu geliştirmek için sürekli müfredat güncellemeleri, endüstri ortaklıkları ve pratik eğitim fırsatları sağlamayı amaçlayan CyberAgent projesinin alaka düzeyini vurgulamaktadır.

KOBİ'lere özel konular

Konu/Beceri	Sayı
KOBİ'ler için temel siber güvenlik	91
KOBİ'ler için veri koruma ve gizlilik	75
Programa hiçbir KOBİ'nin özel konusu veya becerisi dahil edilmemiştir	**64**
KOBİ'ler için olay müdahalesi	58
KOBİ'ler bağlamında risk değerlendirmesi ve yönetimi	53
KOBİ'ler için siber güvenlik politikası geliştirme	46

Temel siber güvenlik ilkelerine ve veri korumasına güçlü bir vurgu vardır. En sık bahsedilen konular olan KOBİ'ler için Temel Siber Güvenlik ve KOBİ'ler için Veri Koruma ve Gizlilik, eğitimcilerin KOBİ'leri verilerini koruyacak ve temel siber güvenlik kavramlarını anlayacak bilgilerle donatmaya öncelik verdiğini gösteriyor. "Hiçbir KOBİ'nin belirli konusu veya becerileri programa dahil edilmemiştir" numarası, Küçük ve Orta Ölçekli İşletmeler (KOBİ'ler) için özel içerikle ilgili bazı siber güvenlik eğitim programlarında bir boşluk olduğunu göstermektedir. Özellikle KOBİ'lerin karşılaştığı zorluklar ve tehditler göz önüne alındığında, siber güvenlik eğitimlerinde iyileştirilmesi gereken kritik bir alanı vurgulamaktadır.

KOBİ'ler genellikle sınırlı kaynaklarla çalışır ve özel siber güvenlik uzmanlığına erişemeyebilir, bu da onları siber tehditlere karşı özellikle savunmasız hale getirir. Siber güvenlik eğitim programlarında KOBİ'lere özel içeriğin bulunmaması, bu programların KOBİ'lerin farklı ihtiyaçlarını tam olarak karşılayamayabileceğini ve potansiyel olarak siber saldırılara karşı hazırlıklarında ve dayanıklılıklarında bir boşluk bırakabileceğini düşündürmektedir. Bu boşluğu gidermek, daha küçük işletme operasyonlarına göre uyarlanmış risk değerlendirmesi, uygun maliyetli siber güvenlik uygulamaları ve sınırlı kaynaklarla etkili bir siber güvenlik politikası geliştirme stratejileri gibi KOBİ'lerin siber güvenlik ihtiyaçlarını karşılamak için özel olarak tasarlanmış konuların ve becerilerin entegrasyonunu gerektirir.

KOBİ çalışanlarında beceri açığı

Beceri/Konu	Sayı
Tehdit algılama ve müdahale	103
Bulut güvenliği uzmanlığı	87
Olay müdahalesi ve kurtarma	69
Veri gizliliği ve koruması	67

Risk yönetimi ve analizi	63
Gelişmekte olan teknolojiler	58
Ağ güvenliği	41
Uyumluluk ve mevzuat bilgisi	36

Analiz, çalışanların kilit alanlarda becerilerden yoksun olduğunu ve Tehdit algılama ve müdahalenin en sık dile getirilen unsurlar olduğunu ortaya koymaktadır. Bu, öğrencileri siber güvenlik tehditlerini belirlemeye ve bunlara yanıt vermeye hazırlamanın önemini vurgulamaktadır. Bulut güvenliği uzmanlığı, bulut teknolojilerine olan güveni ve bulut ortamlarını çalışanlardan korumak için özel bilgi ihtiyacını gösteren ikinci sırada yer alıyor. Olay müdahalesi ve kurtarma, Veri gizliliği ve koruması ve Risk yönetimi ve analizi de değerlidir. Gelişen teknolojilerle ilgili olarak, alandaki en son gelişmelerden haberdar olma ihtiyacının bir açık alanı olmadığı düşünülmektedir. Siber güvenlik eğitim programlarının çoğunun bir parçası olan temel bir alan olan Ağ güvenliği için de aynı şey geçerlidir. O noktadaki eğitimlerin etkinliğini gösterir.

Tehdit

Tehdit	**Sayı**
Yapay zeka odaklı siber saldırılar	117
Fidye yazılımı saldırıları	96
Kimlik avı ve sosyal mühendislik	87
Bulut güvenliği ihlalleri	82
IoT güvenlik açıkları	75
Deepfake tehditleri	51
İçeriden gelen tehditler	25

Analiz, en sık bahsedilen yeni ortaya çıkan siber güvenlik tehdidi olarak yapay zeka odaklı siber saldırılara önemli bir odaklanma olduğunu ortaya koyuyor ve bu da yapay zeka tarafından desteklenen siber tehditlerin karmaşıklığı ve karmaşıklığı konusunda bir endişeye işaret ediyor. Fidye yazılımı saldırıları, kimlik avı ve sosyal mühendislik de KOBİ'ler için bu saldırı vektörlerinin varlığını göstererek üst sıralarda yer aldı. Bulut güvenliği ihlalleri ve IoT güvenlik açıkları, bulut hizmetlerinin güvenliği ve genişleyen Nesnelerin İnterneti ile ilgili endişeleri vurgulayarak, KOBİ'ler için çeşitli ve dağıtılmış teknolojik ekosistemleri korumadaki zorlukları yansıtıyor. Deepfake tehditleri ve içeriden gelen tehditler büyük tehdit vektörleri olarak kabul edilmez. En önemli 5 konuyu kapsayan bir eğitim programı, öğrencileri ve KOBİ çalışanlarını karşılaşılan tehditlerle başa çıkmak için daha iyi donatabilir.

Yükselen trendler

Alan	**Sayı**
Siber Güvenlikte Yapay Zeka ve Makine Öğrenimi	160
Dijital Kimlik ve Gizlilik	96
Etik Hacking ve Savunma Becerileri	82
Kuantum Bilişim Tehditleri	67

Merkezi olmayan güvenlik sistemleri (ör. Blockchain)	52
Sosyal becerilere ve disiplinler arası eğitime odaklanın	47

Siber Güvenlikte Yapay Zeka ve Makine Öğrenimine en sık bahsedilen alan olarak güçlü bir vurgu yapılmakta olup, bu teknolojilerin siber güvenlik önlemlerini geliştirmedeki önemini ve bu alanlarda yetenekli profesyonellere olan ihtiyacı yansıtmaktadır. Dijital Kimlik ve Gizlilik, dijital kimliklerin korunmasının ve gizliliğin sağlanmasının önemini vurgulayan bir diğer önemli odak noktasıdır. Etik Hacking ve Savunma Becerileri puanı, profesyonellerin güvenlik açıklarını belirlemelerini ve saldırılara karşı etkili bir şekilde savunma yapmalarını sağlayan pratik, uygulamalı becerilere olan talebi gösterir. Kuantum Hesaplama Tehditleri, blok zinciri teknolojisi ve yumuşak Beceriler ve Disiplinlerarası Eğitim gibi merkezi olmayan güvenlik sistemleri yükselen trendler olarak kabul edilmedi. Yanıtların dağılımı, siber güvenlik alanının çeşitliliğini ve profesyonelleri mevcut ve gelecekteki zorlukların üstesinden gelmek için çeşitli beceri ve bilgilerle hazırlamanın önemini vurgulamaktadır. Ancak yapay zeka konusu, listenin en üstüne güveniyor.

Toplumsal cinsiyet eşitliği

Kadınların Yüzdesi	Yanıt Sayısı
%10'dan az	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
%75'ten fazla	3

Siber güvenlik eğitim programlarındaki kadınların yüzdesi, cinsiyet çeşitliliğinde bir eşitsizlik olduğunu ortaya koyuyor ve yanıtların çoğu düşük kadın katılımı gösteriyor. Ayrıntılı olarak, 79 yanıt kadınların katılımını %10 ila %25 arasında yerleştirdi ve 57 yanıt bu oranın %10'dan az olduğunu gösterdi. Bazı programlarda orta düzeyde bir cinsiyet çeşitliliği önerilmektedir ve 43 katılımcı kadınların katılım oranının %26 ila %50 arasında olduğunu tahmin etmektedir. Bununla birlikte, yüksek oranda kadın katılımcıya sahip programlar oldukça nadirdir, %51 ila %75 aralığını gösteren sadece 8 yanıt ve %75'ten fazlasını tahmin eden minimum 3 yanıt sayısı ile kanıtlanmıştır. Bu veriler, siber güvenlik eğitim programlarında cinsiyet çeşitliliğini sağlamanın zorluğunun altını çiziyor ve rapor edilen programların çoğunda kadın katılımında önemli bir boşluğu vurguluyor.

Toplumsal cinsiyet girişimleri

Yanıt	Yanıt Sayısı
Evet	30
Hayır	160

Veriler, ankete katılanların önemli bir çoğunluğunun, yani toplamda 160 kişinin, kadınların siber güvenlik eğitimine katılımını teşvik etmek için belirli girişimler veya stratejiler kullanmadığını gösteriyor. Sadece 30 katılımcı bu tür önlemlerin uygulandığını doğruladı. Bu, hedeflenen girişimler yoluyla kadınların siber güvenlik eğitimine katılımını artırmaya yönelik bir miktar

farkındalık ve çaba olsa da, programların çoğunun cinsiyet çeşitliliğini ele almak için henüz belirli stratejilere öncelik vermeyebileceğini veya uygulamayabileceğini göstermektedir. Hedeflenen girişimlerin bu eksikliği, önceki soruya verilen yanıtlarda belirtildiği gibi, kadınların katılımının düşük yüzdelerine katkıda bulunabilir.

Toplumsal cinsiyet kapsayıcı eğitim

Yanıt	Yanıt Sayısı
Evet	47
Hayır	44
Emin	72
Benimle alakalı değil	27

Sonuçlar, siber güvenlikte cinsiyet kapsayıcı eğitim modüllerinin mevcudiyeti konusunda katılımcılar arasında bölünmüş bir görüş olduğunu göstermektedir. 72 katılımcıdan oluşan en büyük grup, cinsiyet içeren materyallerin varlığı hakkında net bir fikir birliği veya bilgi eksikliğini gösteren belirsizliği ("Emin Değilim") ifade etti. Yeterince cinsiyet içeren modül olduğuna inananlar (47 yanıtları) ile inanmayanlar (44 yanıtları) arasında neredeyse eşit bir bölünme var. Ek olarak, 27 katılımcı sorunun deneyimleriyle veya bağlamlarıyla ilgili olmadığını düşünüyor.

Bu bölüm, siber güvenlik eğitim içeriğinin kapsayıcılığı hakkında devam eden tartışmaları ve çeşitli algıları yansıtmaktadır. Belirsiz yanıtların sayısının yüksek olması, siber güvenlik eğitim ve öğretim ekosisteminde toplumsal cinsiyeti kapsayıcı eğitim kaynaklarının farkındalığı veya erişilebilirliği konusunda potansiyel bir boşluğu vurgulamaktadır.

Toplumsal cinsiyet kapsayıcılığının önündeki engeller

Engel	Sayı
Stereotipler veya kültürel normlar	107
Siber güvenlikteki fırsatlar hakkında farkındalık eksikliği	86
Mentorluk veya rol model eksikliği	74
İş-yaşam dengesi zorlukları	60
Sektörde algılanan cinsiyet yanlılığı	58

Ankete katılanların algıladığı gibi, kadınların siber güvenliğe katılımının önündeki en önemli engeller, klişeler veya kültürel normlar (107 söz) ve siber güvenlik fırsatları hakkında farkındalık eksikliğidir (86 söz). Bu iki engel, toplumsal algıların ve kariyer yolları hakkında yetersiz bilginin, kadınların siber güvenlik alanına girişini önemli ölçüde engellediğini göstermektedir. Mentorluk veya rol model eksikliği ve iş-yaşam dengesi zorlukları da önemli engellerdir ve kadınların katılımını teşvik etmede destek ağlarının ve esnek çalışma ortamlarının önemini vurgulamaktadır. Ek olarak, sektörde algılanan cinsiyet yanlılığı, alanı kadınlar için daha sıcak ve eşitlikçi hale getirmek için kültürel ve sistemik değişikliklere duyulan ihtiyaca işaret ediyor.

Çeşitliliği ve kapsayıcılığı teşvik etmek için özel program

Yanıt	Yanıt Sayısı
Evet	44
Hayır	85
Emin değilim	61

Veriler, ankete katılan kurumların önemli bir bölümünün, 85 yanıtla, siber güvenlik eğitiminde kadınlar için çeşitliliği ve kapsayıcılığı teşvik etmek için belirli politikalara veya programlara sahip olmadığını ortaya koyuyor. Bu arada, 44 katılımcı, kurumlarının bu tür girişimleri uyguladığını belirterek, bu alanda cinsiyet çeşitliliğini ele almaya yönelik bir yaklaşımı vurguladı. Bununla birlikte, 61 katılımcının kayda değer bir kısmı, kurumlarının bu tür politikalara veya programlara sahip olup olmadığından emin değil, bu da mevcut çeşitlilik ve kapsayıcılık çabalarına ilişkin potansiyel bir iletişim veya farkındalık eksikliğine işaret ediyor. Ayrıca, bu karışık yanıt, bazı kurumlar siber güvenlik eğitiminde kapsayıcılığa yönelik adımlar atarken, hem çeşitlilik programlarının uygulanmasında hem de öğretim üyeleri, personel ve öğrenciler arasında bu tür girişimlerin farkındalığında önemli bir boşluk kaldığını göstermektedir.

İyileştirmeler için öneri

Öneri	Sayı
Başarılı kadın siber güvenlik uzmanlarının görünürlüğünün artırılması	95
Daha fazla kadın siber güvenlik eğitmeni veya eğitim personeli	89
Burs veya teşvikler sunun	81
Mentorluk fırsatları	49
Cinsiyet önyargılarından kaçınan eğitim içeriği	33
Kapsayıcılığı desteklemek için politikaları düzenli olarak güncelleyin	31
Cinsiyet kapsayıcı vaka çalışmaları ve senaryolar	24
Kişiye özel eğitim programları	21
Kadınlara özel daha fazla eğitim seansı	18

Siber güvenlik eğitimini daha toplumsal cinsiyeti kapsayıcı hale getirme önerileriyle ilgili yanıtların analizi, birkaç temel stratejinin önemi konusunda güçlü bir fikir birliği ortaya koyuyor. 95 sözle en çok onaylanan öneri, başarılı kadın siber güvenlik uzmanlarının görünürlüğünün artmasıdır. Bu, rol modellerin ve hevesli figürlerin kadınlara siber güvenlik alanında kariyer yapmaları için ilham vermedeki kritik rolünün altını çiziyor. Arkasında, 89 sözle, daha fazla kadın siber güvenlik eğitmeni veya eğitim personeli için yapılan çağrı, eğitim işgücü içinde temsil edilme ihtiyacını vurguluyor. Burs veya teşvik sunmak, 81 söz almak, alanı finansal olarak daha erişilebilir ve kadınlar için çekici hale getirmek için çok önemli olarak tanımlanıyor. Ankete katılan 49 kişi tarafından belirtilen mentorluk fırsatları, alanında deneyimli profesyonellerin rehberliğinin ve desteğinin önemini vurgulamaktadır. Cinsiyet önyargılarından kaçınan eğitim içeriğine ve kapsayıcılığı desteklemek için düzenli olarak güncellenen politikalara duyulan ihtiyaç, çeşitliliği yansıtan ve teşvik eden müfredat ve politika düzenlemelerinin gerekliliğine işaret ediyor.

KOBİ'ler için saha araştırması analizi

Demografik:

Anket, ortakların ülkelerinden yanıtlar aldı. Romanya en yüksek katılımcı sayısına (28) sahipken, onu Norveç (23) ve ardından her biri 21 katılımcıyla Litvanya, İspanya ve Belçika izliyor. Finlandiya ve Türkiye'nin de 20'şer yanıt ile önemli sayıda yanıtı var ve Polonya 19 yanıtlayanlarla hemen arkasında.

Şirket sektörü

Firma Sektörü	Sayı
Bilişim	18
Eğitim	6
İnşaat	4
Danışmanlık	4
Siber güvenlik	4

Veriler, BT sektöründen güçlü bir temsile işaret ediyor ve 18 katılımcı şirketlerini bu sektörde faaliyet gösteriyor olarak tanımlıyor. Eğitim, İnşaat, Danışmanlık ve Siber Güvenlik sektörleri de her biri 4 ile 6 arasında değişen sayılara sahip dikkate değer temsillere sahiptir. İlk beşin ötesinde, anketin çeşitli sektörlerdeki geniş yaklaşımını gösteren, daha az sayıya sahip uzun bir sektör kuyruğu var.

Yanıtlayanların profili

Şirketteki Pozisyonu	Sayı
Müdür	48
Yönetici/Sahip	35
Teknik (Mühendis/Geliştirici/Analist)	27
Başka	25
Koordinatör/Yönetici	8
Satış/Pazarlama	8
Uzman/Uzman	8
Çalışan	8
Danışman	3
Eğitim/Öğretim	2
Finans/Muhasebe	1
Proje yönetimi	1
HR	1
Toplam	**175**

Farklı bir profesyonel kitleye sahip çok çeşitli iş unvanları ve organizasyonel hiyerarşiler içinde çeşitli seviyeleri kapsayan geniş bir katılımcı yelpazesini gösteren "Çalışan" ve "Direktör" gibi geniş bir pozisyon paneli vardır. Siber güvenlik, bireyleri şirketlerdeki farklı roller ve sorumluluklar arasında meşgul eden kesişen bir konudur.

Cinsiyet

Ankete katılanlar arasındaki cinsiyet dağılımı, erkeklerin (102) kadınlara (69) kıyasla daha yüksek temsil edildiğini ortaya koymaktadır ve katılımcıların küçük bir kısmı (4) cinsiyetlerini açıklamamayı tercih etmektedir. Bu dağılım, anketin temsil ettiği alanda bir cinsiyet farkı olduğunu gösteriyor ve bu, erkek egemenliğinin sıklıkla bildirildiği siber güvenlik ve teknoloji sektörlerindeki daha geniş eğilimleri yansıtıyor. Bununla birlikte, kadın katılımcıların önemli sayısı, kadınların alana anlamlı bir şekilde katıldığını gösteriyor ve sektörün cinsiyet çeşitliliğinde devam eden değişikliklere işaret ediyor. Cinsiyet farkı aşikar olsa da, yanıtlardaki çeşitlilik aynı zamanda siber güvenlikte kademeli olarak değişen bir manzaraya işaret ediyor.

Ülkelere göre cinsiyet dağılımı

Ülke	Dişi	Erkek	Söylememeyi tercih ederim
Belçika	10	10	1
Finlandiya	9	11	0
Litvanya	9	12	0
Norveç	8	15	0
Polonya	8	9	2
Romanya	12	16	0
İspanya	6	14	1
Türkiye	7	13	0

Tablo, farklı ülkeler arasındaki cinsiyet dağılımını göstermektedir. Erkek katılımcıların sayısı, daha önce tartışılan genel cinsiyet dağılımıyla tutarlı olarak, her ülkede kadın katılımcılardan fazladır. Bununla birlikte, Belçika gibi bazı ülkelerde eşit sayıda erkek ve kadın katılımcı (her biri 10) ve Polonya gibi bazı ülkelerde erkekler (9) ve kadınlar (8) arasında daha yakın bir dağılım olduğu ve az sayıda katılımcı cinsiyetlerini söylememeyi tercih ettiği (2) ile fark ülkeye göre değişmektedir. Romanya ve Norveç gibi ülkeler genel olarak daha fazla sayıda katılımcıya sahiptir ve daha yüksek bir erkek-kadın oranını korumaktadır. Bu cinsiyet-ülke dağılımı, siber güvenlik alanındaki hem cinsiyet eşitsizliklerini hem de coğrafi çeşitliliği vurgulayarak ankete katılanların demografik yapısının incelikli bir şekilde anlaşılmasını sağlıyor.

Şirket büyüklüğü

Şirket Büyüklüğü	Sayı
10 çalışana kadar	64
11-50	60
51-250	51

Anket yanıtları, katılımcılar arasında önemli sayıda küçük ve orta ölçekli işletmeye işaret ediyor. En büyük grup, 10 çalışana kadar olan şirketler (64 katılımcı), ardından 11 ila 50 çalışanı olan şirketler (60 katılımcı) ve ardından 51 ila 250 çalışanı olan şirketler (51 katılımcı) geliyor.

Ankete katılanlar arasında daha küçük şirketlerin baskın olması, KOBİ'lerin özel ihtiyaçlarını ve kısıtlamalarını ele alan özel siber güvenlik çözümlerinin önemini vurguluyor.

Bilgi düzeyi

Siber Güvenlik Bilgi Düzeyi	Sayı
Ara	85
Acemi	64
İleri	26

Anket yanıtları, ankete katılanların çoğunluğunun çalışanlarının mevcut siber güvenlik bilgi düzeyini "Orta" (85) olarak değerlendirdiğini, bunu "Başlangıç" düzeyinde değerlendirenlerin (64) ve daha küçük bir kısmının çalışanlarını "İleri" siber güvenlik bilgisine sahip olarak gördüğünü (26) gösteriyor.

Bu dağılım, temsil edilen kuruluşlarda siber güvenlik becerilerinde büyüme ve gelişme için önemli bir potansiyel olduğunu göstermektedir. "Orta" ve "Başlangıç" seviyelerinin çoğu, bu çalışanların siber güvenlik bilgi tabanını yükseltmek için sürekli eğitim ve öğretim girişimlerinin gerekliliğine işaret ediyor. Farklı bilgi seviyelerine hitap eden hedefli siber güvenlik eğitim programları için bir fırsatı vurgular ve temel siber güvenlik ilkelerinin yeni başlayanlar tarafından iyi anlaşılmasını sağlar.

Daha az sayıda olsa da, ileri düzeyde bilgiye sahip çalışanların varlığı, bazı kuruluşlarda temel bir siber güvenlik uzmanlığı katmanına işaret ettiği için cesaret vericidir.

Şirket büyüklüğüne dayalı bilgi düzeyi.

Şirket Büyüklüğü	İleri	Acemi	Orta
10 çalışana kadar	6	25	33
11-50	10	20	30
51-250	10	19	22

Tablo, siber güvenlik bilgi düzeylerinin (İleri, Başlangıç, Orta) farklı şirket boyutlarına nasıl dağıldığını gösterir. Küçük Şirketler (10 çalışana kadar) "Orta" düzeyde siber güvenlik bilgisine ve ardından "Başlangıç" seviyesine doğru bir eğilim göstermektedir. Bu, küçük şirketlerin siber güvenlik konusunda bir miktar anlayışa sahip olsa da, başlangıç seviyesinde hala önemli bir kısım olduğunu ve bu da iyileştirme için yer olduğunu ve daha temel eğitime ihtiyaç duyulduğunu gösteriyor. Orta Ölçekli Şirketler (11-50 çalışan), "Orta" bilgi için hafif bir tercih ile bilgi seviyeleri arasında dengeli bir dağılıma sahiptir. Bu, biraz daha büyük kuruluşlarda siber güvenlik eğitimine daha yapılandırılmış bir yaklaşımı yansıtabilir, ancak benzer şekilde hem gelişmiş anlayış hem de temel öğrenme ihtiyaçlarının varlığını gösterir. Daha büyük KOBİ'ler (51-250 çalışan), eşit sayıda ileri ve başlangıç seviyesine ve biraz daha düşük orta düzey bilgiye sahip orta ölçekli şirketlere benzer bir model izlemektedir.

Tüm şirket boyutlarında, "Orta" düzeyde siber güvenlik bilgisi en yaygın olanıdır.

Siber güvenlik görevleriyle uğraşan çalışanlar

Sayı	Sayı
1-5	88
0	22
6-10	17
21+	12
11-20	5

Siber Güvenlikte Çalışan Çeşitliliği	Sayı
0-4	113
5-9	17
10-14	13
20-24	4
25-50	6
+100	9

Tablolar, farklı kuruluşlar arasında siber güvenlikle ilgili iş yapan çalışan sayısının dağılımını göstermektedir. Siber güvenlik sorumluluklarının farklı çalışan sayıları arasında nasıl dağıtıldığına dair daha net bir görünüm sunar. Yanıtların büyük çoğunluğu 0-4 aralığındadır, bu da çok küçük siber güvenlik ekiplerine sahip çok sayıda kuruluş olduğunu veya hatta özellikle siber güvenliğe adanmış olmadığını gösterir. Daha yüksek aralıklara geçtikçe, siber güvenliğe adanmış 100'den fazla çalışanı olan kuruluşlarda bir miktar canlanma ile frekansta önemli bir düşüş var. Bu şirketlerin ana meslekleri olarak siber güvenlik alanında çalıştıkları gerçeğiyle açıklanmaktadır.

Ayrıntılı olarak, veriler, siber güvenlik ekiplerinin boyutunda geniş bir aralık olduğunu gösteriyor, en yaygın boyut tek bir çalışan, ardından birçok kuruluşun özel siber güvenlik personeline minimum düzeyde güvendiğini veya hiç güvenmediğini gösteren özel bir siber güvenlik çalışanı yok. Ekip büyüklüğü arttıkça frekansta gözle görülür bir azalma olur.

Dağılım, önemli sayıda küçük ve orta ölçekli işletmenin (KOBİ) siber güvenliğe ayrılmış yeterli kaynağa sahip olmayabileceği ve onları daha büyük risklere maruz bırakabileceği siber güvenlik iş gücü tahsisinde potansiyel bir boşluğu vurgulamaktadır. Bazı kuruluşlarda daha büyük ekiplerin varlığı, belirli sektörlerde veya daha büyük şirketlerde siber güvenliğin öneminin kabul edildiğini göstermektedir.

Siber Güvenlikte Kadınlar

Siber Güvenlikte Kadın Yelpazesi	Sayı
0	78
1-5	57
6-10	8
11-15	4
16-20	1

"Bu çalışanların kaçı kadın?" sorusunun sonuçları, KOBİ'lerdeki siber güvenlik iş gücünde önemli bir cinsiyet farkını vurgulamaktadır. En çarpıcı gözlem, şirketlerin çoğunluğunun, toplamda 78'inin, siber güvenlik rollerinde hiç kadın olmadığını bildirmesi. Bu, ankete katılan KOBİ'ler arasında bu kritik alanda kadınların yetersiz temsil edilmesinin yaygın bir sorununa işaret ediyor. Siber güvenlik rollerindeki kadın sayısı arttıkça bu sayının kademeli olarak azaldığı ve 31 şirketin bu pozisyonda bir kadına sahip olduğu belirtiliyor. Siber güvenlik rollerinde 10 veya daha fazla kadına sahip birkaç şirketin varlığı, olumlu olsa da, normdan ziyade bir istisna olmaya devam ediyor. Bu örnekler, daha büyük siber güvenlik ekiplerine sahip kuruluşları veya siber güvenlik iş gücünde cinsiyet çeşitliliğine özel olarak odaklanan kuruluşları temsil edebilir. Kadınları siber güvenlik alanında kariyer yapmaya teşvik etmeyi ve desteklemeyi amaçlayan girişimlere duyulan ihtiyacın altını çiziyor. Siber güvenlik rollerinde hiç kadın olmayan önemli sayıda şirket, sektörde cinsiyet çeşitliliğini ve kapsayıcılığı teşvik etmek için kritik bir müdahale alanını vurgulamaktadır. Bu cinsiyet uçurumunu kapatmak, siber güvenlik zorluklarının üstesinden gelmede daha çeşitli bakış açılarına katkıda bulunabilir.

Harici hizmetlerin kullanımı

Yanıt	Sayı
Hayır	115
Evet	60

Yanıtlar, KOBİ'lerin siber güvenliğe nasıl yaklaştığının önemli bir yönünü ortaya koyuyor. Ankete katılan şirketlerin çoğunluğu, 175 şirketten 115'i, siber güvenlik çalışmaları için harici hizmetler kiralamadıklarını belirtiyor. Bu, KOBİ nüfusunun büyük bir kesiminde siber güvenlik çabalarını dahili olarak yönetmek için bir tercih veya gereklilik olduğunu göstermektedir. Bütçe kısıtlamaları, siber güvenlik uygulamaları üzerinde algılanan kontrol veya mevcut dahili kaynaklarının siber güvenlik ihtiyaçlarını karşılamak için yeterli olduğu inancı gibi çeşitli faktörler bu eğilimi yönlendirebilir. Bu durum, CyberAgent projesini çalışanı temel beceri ve bilgilerle donatmak için son derece alakalı hale getiriyor.

60 şirket, siber güvenlik görevleri için harici hizmetler işe aldığını bildirdi. Bu grup muhtemelen, özel becerilere erişmek, en son siber güvenlik tehditleri ve karşı önlemleri konusunda güncel kalmak veya dahili yeteneklerini desteklemek gibi dış kaynak kullanımının faydalarını kabul ediyor. Harici hizmetleri işe alma kararı, özellikle sınırlı kaynaklara sahip KOBİ'ler için tamamen şirket içinde yönetilmesi zor olabilen siber güvenlik tehditlerinin karmaşıklığının anlaşılmasını da yansıtabilir.

Bu bölünme, KOBİ'ler arasında siber güvenlik stratejisinde, siber güvenlik işlevlerinin iç yönetimi ile dış kaynak kullanımı arasında denge kuran bir farklılığı vurgulamaktadır. Farklı kuruluşların siber güvenlik çabaları için harici destek alıp almama konusundaki kararlarını etkileyen çeşitli ihtiyaçlara, yeteneklere ve kaynaklara sahip olabileceğini kabul ederek siber güvenliğe özel bir yaklaşımın önemini vurgulamaktadır.

Eğitim programlarının etkinliği

Yanıt	Sayı
1 (Etkisiz)	8
2	38
3	79
4	39
5 (Çok Etkili)	11

Yanıtlar, öğrencileri KOBİ'lerde gerçek dünyadaki siber güvenlik zorluklarına hazırlamada mevcut eğitim programlarının etkinliğine ilişkin algılar hakkında fikir vermektedir. Ankete katılanların çoğunluğu, 79 sayıyla, mevcut eğitim programlarının etkinliğini '3' olarak değerlendirdi ve bu da etkinliklerinin nötr veya ılımlı bir şekilde algılandığını gösterdi. Bu, bu programlara bir miktar güven olsa da, iyileştirme için önemli bir alan olduğunu göstermektedir. Yanıtlar ayrıca, ölçeğin alt ucuna doğru bir eğilim göstermekte olup, '2' 38 sayı almakta ve bu eğitim programlarının etkinliği konusunda şüpheciliğe işaret etmektedir. Uç noktalarda, '1' (etkisiz) en az sayıda seçim aldı (8 sayım) ve '5' (çok etkili) biraz daha fazla (11 sayım) aldı. Bu, çok az sayıda katılımcının mevcut eğitim programlarını öğrencileri KOBİ'lerdeki siber güvenlik zorluklarına hazırlamada tamamen etkisiz veya çok etkili olarak gördüğünü göstermektedir. '4' için dengeli yanıt sayısı (39 sayı), katılımcıların önemli bir bölümünün eğitim programlarını önemli sınırlamalar olmasa da nispeten etkili olarak gördüğünü göstermektedir. Mevcut eğitim programları, KOBİ'lerde gerçek dünyadaki siber güvenlik zorluklarına bir miktar hazırlık sağlarken, verilen eğitim ile sektörün ihtiyaçları arasında bir boşluk var. Bu boşluk, siber güvenlik tehditlerindeki evrimin hızı, becerilerin pratik uygulaması veya KOBİ'lerin karşılaştığı zorlukların özgüllüğü gibi çeşitli faktörlerden kaynaklanıyor olabilir.

Siber güvenlik eğitiminde en önemli 3 alan

Kategori	Sayı
Tehdit algılama ve müdahale	102
Risk yönetimi ve analizi	81
Olay müdahalesi ve kurtarma	72
Veri gizliliği ve koruması	68
Bulut güvenliği uzmanlığı	51
Ağ güvenliği	46
Uyumluluk ve mevzuat bilgisi	31
Gelişmekte olan teknolojiler	24

Yanıtların analizi, "Tehdit algılama ve müdahale"nin 102 sayımla siber güvenlik eğitiminde en önemli alan olarak kabul edildiğini ortaya koyuyor ve bu da KOBİ'lerde gerçek dünyadaki siber güvenlik zorluklarını ele almanın önemine dair güçlü bir inancı gösteriyor. Bu alanı, sırasıyla 81 ve 72 sayımla "Risk yönetimi ve analizi" ve "Olay müdahalesi ve kurtarma" yakından takip ediyor ve riskleri anlamaya ve olaylara etkili bir şekilde yanıt verebilmeye verilen değeri vurguluyor. "Veri gizliliği ve koruması", veri koruma yasalarının artan önemini ve dijital çağda kişisel ve hassas bilgilerin korunması ihtiyacını yansıtan önemli bir vurgu yapmaktadır. "Bulut güvenliği uzmanlığı", muhtemelen bulut hizmetlerinin giderek daha fazla benimsenmesi ve sundukları benzersiz güvenlik zorlukları nedeniyle 51 katılımcı tarafından kilit bir alan olarak tanımlanıyor. 46 sayımla ağ güvenliği, ağ tabanlı tehditlere karşı güçlü savunma ihtiyacının altını çizen temel bir endişe kaynağı olmaya devam ediyor. "Uyumluluk ve mevzuat bilgisi" ve "Gelişmekte olan teknolojiler" daha az önemli görülmektedir.

Yetkinlikler ve bilgi

Yetkinlik ve Bilgi Alanı	Temel (%)	Yüksek İhtiyaç (%)	Orta İhtiyaç (%)	Düşük İhtiyaç (%)	Gerekli Değil (%)
Veri Gizliliği ve Koruması	38.29	38.29	13.14	10.29	0.00*
Risk Değerlendirmesi ve Yönetimi	34.86	36.00	24.00	4.57	0.57
Olay Müdahalesi ve Kurtarma	33.14	38.86	19.43	8.00	0.57
İletişim Becerileri	32.57	35.43	22.29	8.00	1.71
Teknik Bilgi	30.29	32.00	26.29	8.57	2.86
Tehdit İstihbaratı ve İzleme	29.71	37.14	24.00	8.57	0.57
Politika Geliştirme ve Uygulama	24.00	37.14	24.00	12.57	2.29

*: "Veri Gizliliği ve Koruması" için "Gerekli Değil" yüzdesi mevcut değil (NaN), bu da tüm katılımcıların bu alanı en azından bir miktar ihtiyaç olarak görmesinden kaynaklanıyor olabilir, bu nedenle %0 olarak kabul edilebilir.

Tablo, her bir yetkinlik ve bilgi alanı için, önemlerini 1 (gerekli değil) ile 5 (temel) arasında bir ölçekte derecelendiren anket yanıtlarından elde edilen ortalama puanları sunar. Bu puanlar, yanıtlayanların alandaki farklı alanlara nasıl öncelik verdiğine dair nicel bir fikir verir.

Bu tablo, her bir yetkinlik ve bilgi alanının yanıtlayanlar tarafından nasıl değerlendirildiğinin net bir dökümünü sağlar. "Veri Gizliliği ve Koruması" ve "Risk Değerlendirmesi ve Yönetimi" gibi alanlar, alandaki kritik önemlerini yansıtan en yüksek "Temel" derecelendirme yüzdesine sahiptir. Buna karşılık, "Politika Geliştirme ve Uygulama", yanıtların daha geniş bir dağılımını göstermekte ve önemine ilişkin daha çeşitli bir algıya işaret etmektedir. Sonuçlar, teknik bilgiye, tehdit farkındalığına ve olaylara yanıt verme becerisine güçlü bir vurgunun yanı sıra etkili iletişim ve veri koruma uygulamalarına duyulan önemli ihtiyacı vurgulamaktadır.

Ortaya çıkan siber güvenlik tehditleri

Ortaya Çıkan Siber Güvenlik Tehdidi	Frekans
Kimlik avı ve sosyal mühendislik	105
Yapay zeka odaklı siber saldırılar	95
Fidye yazılımı saldırıları	90
Bulut güvenliği ihlalleri	60
Deepfake tehditleri	57
IoT güvenlik açıkları	44
İçeriden gelen tehditler	31

Kimlik avı ve sosyal mühendislik, yapay zeka odaklı siber saldırılar ve fidye yazılımı saldırılarının da önemli ölçüde ilgi görmesiyle en acil tehditler olarak kabul ediliyor. Bu, KOBİ'ler arasında hem geleneksel hem de ortaya çıkan siber tehditlere karşı korunma ihtiyacı konusunda güçlü bir farkındalık olduğunu gösteriyor. Bulut güvenlik ihlalleri ve deepfake tehditleri de vurgulanarak bulut hizmetlerinin güvenliği ve yapay zekanın potansiyel kötüye kullanımı ile ilgili endişeler yansıtılıyor. IoT güvenlik açıkları ve içeriden gelen tehditler de tanımlanıyor, ancak diğer kategorilere göre daha az yakın olarak görülüyorlar. Özellikle, bazı katılımcıların belirli tehditlerden emin olmadıklarını veya iş düzeylerinde fikirleri olmadığını gösteren yanıtlar var, bu da bazı KOBİ'ler arasında ortaya çıkan belirli tehditler hakkında farkındalık veya endişede potansiyel bir boşluk olduğunu gösteriyor.

Siber Güvenlik Bilgi veya Becerilerindeki Boşluk

Siber Güvenlik Bilgi veya Becerilerindeki Boşluk	Frekans
Düşük düzeyde Tehdit Farkındalığı	105
Düşük Seviyede Siber Güvenlik Düzenli Eğitimleri	88
Düşük düzeyde Güvenlik Açığı Değerlendirmesi	80
Düşük Teknik Beceri Seviyesi	71
Düşük düzeyde Politika ve Yönetmelik Anlayışı	50
Düşük Düzeyde Yumuşak Beceriler	37

Çalışanlar arasında siber güvenlik bilgi veya becerilerindeki en önemli boşluklar tehdit farkındalığı, düzenli siber güvenlik eğitimleri, güvenlik açığı değerlendirmesi, teknik beceriler ve politika ve düzenlemelerin anlaşılmasıdır. Bu yanıtların sıklığı, bu belirli alanları ele alan kapsamlı siber güvenlik eğitimi ve öğretimi için çok önemli bir ihtiyacı vurgulamaktadır. Tehdit farkındalığı en önemli boşluk olarak öne çıkıyor ve çalışanların kuruluşlarını etkileyebilecek siber güvenlik tehditlerinin tam olarak farkında olmayabileceğini gösteriyor. Bu boşluk, çalışanların potansiyel tehditleri daha etkili bir şekilde tanımalarına yardımcı olmak için farkındalık programlarının ve eğitimin geliştirilmesinin önemini vurgulamaktadır. Düzenli siber güvenlik eğitimleri de bir boşluk olarak görülüyor ve tek seferlik eğitim oturumları yerine en son siber güvenlik uygulamaları ve tehditleri hakkında sürekli eğitim ve güncelleme ihtiyacına işaret ediyor.

Yükselen trendler

Siber Güvenlik Eğitiminde Yükselen Trendler	Frekans
Siber Güvenlikte Yapay Zeka ve Makine Öğrenimi	134
Dijital Kimlik ve Gizlilik	108
Etik Hacking ve Savunma Becerileri	86
Sosyal becerilere ve disiplinler arası eğitime odaklanın	54
Kuantum Bilişim Tehditleri	39
Merkezi Olmayan Güvenlik Sistemleri (ör. Blockchain)	28

Analiz, önümüzdeki beş yıl için en çok beklenen trend olarak siber güvenlikte yapay zeka ve makine öğrenimine net bir vurgu yapıldığını ortaya koyuyor. Bu, gelişmiş teknolojilerin siber güvenlik savunmasını geliştirmedeki ve yeni güvenlik çözümleri geliştirmedeki rolünün giderek daha fazla kabul gördüğünü gösteriyor. Bu kategorideki yanıtların yüksek sıklığı, eğitim programlarının siber güvenlik uzmanlarını geleceğe hazırlamak için yapay zeka ve makine öğrenimi bileşenlerini giderek daha fazla birleştirmesi gerekeceğini gösteriyor. Dijital kimlik ve gizlilik, giderek daha çevrimiçi hale gelen bir dünyada kişisel verilerin korunması ve dijital kimliklerin yönetimi ile ilgili endişeleri vurgulayarak en çok beklenen ikinci trend olarak ortaya çıkıyor. Bu eğilim, gizlilik yasalarının, veri koruma tekniklerinin ve kimlik yönetimi çözümlerinin karmaşıklığını kapsayan bir eğitim talebi olduğunu göstermektedir. Etik bilgisayar korsanlığı ve savunma becerileri, siber güvenlikte proaktif savunma stratejilerinin önemini yansıtan üçüncü temel eğilim olarak tanımlanmaktadır. Etik bilgisayar korsanlığına yapılan vurgu, siber güvenlik uzmanlarının kuruluşlarını daha iyi savunmak için saldırganlar gibi düşünmelerini sağlayan eğitime doğru bir kayma olduğunu gösteriyor.

Eğitim programlarının yeterliliği

Yanıt	Frekans
Evet	81
Emin değilim	65
Hayır	29

Katılımcıların mevcut siber güvenlik eğitim programlarının yeterliliği hakkındaki görüşlerini araştıran sorunun analizi, katılımcılar arasında karışık bir bakış açısı ortaya koyuyor. Ankete katılanların çoğunluğunu temsil eden önemli bir bölüm, "Evet" yanıtlarının gösterdiği gibi, mevcut siber güvenlik eğitim programlarının yeterli olduğuna inanıyor. Bu, bazı kişilerin bugün mevcut olan eğitimin kuruluşlarının ihtiyaçlarını karşıladığını veya siber güvenlik eğitiminin neleri içermesi gerektiğine ilişkin beklentileriyle uyumlu olduğunu düşündüğünü göstermektedir. Bununla birlikte, katılımcıların önemli bir kısmı mevcut eğitim programlarının yeterliliğinden "Emin Değil", bu da mevcut eğitim seçenekleri veya mevcut siber güvenlik zorluklarını ele almadaki etkinlikleri hakkında bir dereceye kadar belirsizlik veya bilgi eksikliğini vurguluyor. Bu belirsizlik, siber tehditlerin gelişen doğasına ve eğitim programlarını alandaki en son gelişmelerle güncel tutmanın zorluğuna bağlanabilir. "Hayır" yanıtları, en küçük grubu temsil etmesine rağmen, mevcut eğitim programlarının mevcut siber güvenlik ihtiyaçlarını

karşılamak için yeterli olmadığına dair açık bir endişeye işaret ediyor. Bu grup, eğitimin ortaya çıkan tehditleri, teknolojileri veya metodolojileri kapsayışındaki boşlukları algılayabilir.

Eğitim programlarının kapsayıcılığı

Yanıt	Frekans
Evet	81
Emin değilim	65
Hayır	29

Yanıtların analizi, cinsiyetle ilgili mevcut siber güvenlik eğitim programlarının kapsayıcılığı konusunda farklı bir bakış açısına işaret ediyor. Ankete katılanların çoğu, mevcut eğitimin kapsayıcı olduğunu ve "Evet" yanıtlarında belirtildiği gibi tüm cinsiyetlerin ihtiyaçlarını etkili bir şekilde ele aldığını düşünüyor. Bu, siber güvenlik topluluğunun önemli bir bölümünün mevcut eğitim çabalarının kapsayıcılık ve cinsiyet eşitliğine yönelik adımlar attığına inandığını gösteriyor. Bununla birlikte, çok sayıda katılımcı bu programların kapsayıcılığı konusunda "Emin Değil", bu da siber güvenlik eğitiminin cinsiyet kapsayıcılığı konusunda önemli miktarda belirsizlik veya farkındalık eksikliğine işaret ediyor. Bu yanıt, eğitim sağlayıcılar ve katılımcılar arasındaki iletişim boşluğunu vurgulayabilir veya kapsayıcılık çabalarının amaçlandığı kadar görünür veya etkili olmayabileceğini düşündürebilir. Ankete katılanlar arasında en küçük grubu temsil eden "Hayır" yanıtları, mevcut siber güvenlik eğitiminin tüm cinsiyetlerin ihtiyaçlarını yeterince karşılamadığına dair kritik bir endişeyi vurguluyor. Bu geri bildirim, siber güvenlik eğitim programlarındaki kapsayıcılık çabalarında bir boşluğa işaret ederek, bu programların tüm cinsiyet kimliklerine sahip bireylerin ihtiyaçlarına uygun ve hoş karşılanmasını sağlamak için daha fazla çalışmaya ihtiyaç olduğunu gösteriyor.

3.2. EĞITIM TERCIHLERI VE IHTIYAÇLARI

Saha araştırmasının bulgularına dayanarak, siber güvenlikte yer alan kadınların belirlenen özellikleri ve eğitim ihtiyaçları, öğrenme tercihleri, eğitim ve desteklerinin bir açıklaması aşağıda verilmiştir

Eğitim ihtiyaçlarının belirlenmesi:

Alan 1 - Temel Bilgi ve Beceriler

Siber güvenlik eğitiminde bir öncelik. Özellikle siber güvenlik temelleri ve ağ güvenliği gibi konular. Tehdit algılama ve müdahale, bulut güvenliği uzmanlığı, olay müdahalesi ve kurtarma, veri gizliliği ve koruması, risk yönetimi ve analizi gibi alanlarda önemli boşluklar bulunmaktadır. Eğitim programlarının bu beceri eksikliklerini ele alması gerekir. Ayrıca, KOBİ'lere yönelik içerikler için siber güvenliğe güçlü bir ihtiyaç vardır.

Alan 2 - Uzmanlık Konuları

Bu, geniş bir siber güvenlik tehditleri ve karşı önlemler yelpazesini kapsayan bir eğitim ihtiyacıdır. Tehdit analizi ve yönetimi, kriptografi ve gelişmiş tehdit azaltma teknikleri gibi bazı özel konular vurgulandı. Eğitim, yapay zeka odaklı siber saldırılar, fidye yazılımı saldırıları, kimlik avı ve sosyal mühendislik, bulut güvenliği ihlalleri ve IoT güvenlik açıkları dahil olmak üzere en sık bahsedilen ortaya çıkan tehditlerle ilgili içeriği içermelidir.

Alan 3 - Pratik Uygulama

Uygulamalı laboratuvarlar, vaka çalışmaları ve grup projeleri gibi öğretim yöntemlerinin tercih edilmesi, siber güvenlik eğitiminde pratik, etkileşimli ve gerçek dünya uygulamasının önemini vurgulamaktadır.

Mevcut uygulamalar:

Öğretim yöntemi ile ilgili olarak, vaka çalışmaları, grup projeleri, uygulamalı laboratuvarlar ve dersler gibi çeşitli uygulamaların kullanımını not edebiliriz. Mevcut eğitim programlarında teorik ve pratik yaklaşımların bir karışımı vardır.

Mevcut eğitim programları, temel konulara öncelik verilen bir dizi siber güvenlik konusunu kapsamaktadır. Ancak, bazı programlarda KOBİ'ye özgü içeriğin bulunmadığı belirtilmektedir.

Kapsayıcılık ve cinsiyet dengesi ile ilgili olarak, bazı programlar kadın katılımını artırmak ve toplumsal cinsiyeti kapsayıcı eğitim ortamları yaratmak için girişimler uygulamıştır, ancak bu çabalar azınlıkta görünmektedir.

Zorluklar:

Siber güvenlik eğitiminde karşılaşılan başlıca zorluklar şunlardır:

- Eğitimi çeşitli geçmişlere ve uzmanlık seviyelerine uyacak şekilde uyarlamak, çeşitli beceri ve deneyim olduğu için zordur
- Siber güvenlik tehditlerinin hızlı evrimiyle başa çıkmak için ders materyallerini güncel tutmak. Eğitim materyallerinin sürekli güncellenmesini gerektirir.
- Laboratuvar tesislerindeki sınırlamalar, gerçek dünya simülasyon yetenekleri ve uygulama için gerçekçi siber saldırı senaryolarının oluşturulması nedeniyle pratik eğitim kısıtlamaları
- Özellikle karmaşık teknik içerikle öğrencilerin ilgisini ve motivasyonunu korumak zordur.
- Teorik temellerin endüstri ihtiyaçlarına uygun pratik becerilerle dengelenmesi ile endüstri ve eğitim uyumu bir zorluk teşkil etmektedir.

Eğitim geliştirme için öneri:

- Eğitimi KOBİ ihtiyaçlarına göre uyarlamak: KOBİ'lerin siber güvenlik ihtiyaçlarını karşılamak için özel olarak tasarlanmış konuları ve becerileri entegre etmek.

- Pratik becerileri ve gerçek dünyaya hazır olma durumunu geliştirmek için uygulamalı, etkileşimli öğretim yöntemlerinin kullanımını genişleterek pratik uygulamayı geliştirmek.
- Yapay zeka ve makine öğrenimi, dijital kimlik ve gizlilik ve etik bilgisayar korsanlığı gibi gelişmekte olan trendleri birleştirmek. Artık eğitim programlarında gelecekteki odak noktaları için kilit alanlar olarak kabul edilmektedir.
- Tehdit algılama ve müdahale, bulut güvenliği ve olay müdahalesi gibi çalışanların eksik olduğu alanlara odaklanarak beceri eksikliklerini ele almak, onları zorluklarla yüzleşmeye ve etkili ve esnek CyberAgent olmaya daha iyi hazırlamak.
- Hedeflenen girişimler, mentorluk ve rol modeller aracılığıyla kadın katılımını artırmak için cinsiyet çeşitliliği girişimleri geliştirin.

4. BIR KOBİ SIBER GÜVENLIK DEĞIŞIM TEMSILCISININ YETERLILIK PROFILI

Masa başı ve saha araştırmasının bulgularına dayanarak, CyberAgent'ın beklenen bilgi, beceri ve yetkinlik setine bir örnek. Bu sonuçlar, katılımcıların ilgili siber güvenlik eğitim programlarının sonunda beklenen başarılarını ifade ederek, AYÇ (EQF) seviye 4/5'teki temel bilgi ve becerilerden EQF seviye 6'daki daha ileri ve liderlik odaklı yeteneklere doğru bir gelişim sağlar.

CyberAgent Yeterlilik Profili	Bilgi	Beceri	Yetkinlik
AYÇ 4/5. seviyede	**Siber güvenlik temelleri** - Siber güvenliğin temel kavramları - Siber tehdit türleri (oltalama, fidye yazılımı, ddos saldırıları), saldırı vektörleri - Kurumsal varlıkların korunmasında siber güvenliğin önemi. **Siber güvenlik yasal ve veri çerçevesi** - Siber güvenlik mevzuatı, standartları ve uyumluluk gereksinimleri - Bilgi güvenliği için stratejiler ve politikalar - Veri koruma - Risk yönetimi politikaları	**Güvenlik** - Potansiyel siber güvenlik risklerini ve güvenlik açıklarını belirleyin - Siber tehditlere karşı korunmak için siber güvenlik araçlarını ve yazılımlarını kullanın - Temel siber güvenlik uygulamalarının pratik uygulamasını, güvenli parola oluşturmayı, güvenli taramayı, e-posta güvenliğini ve hassas verilerin güvenli bir şekilde işlenmesini teşvik edin	**Risk yönetimi ve azaltma** - Potansiyel güvenlik tehditlerini değerlendirin ve azaltın **Siber güvenlik konularında etkili iletişim** - Siber güvenlik konularında etkin iletişim kurabilme, - Tehditleri ve ihlalleri kurum içindeki uygun kanallara bildirmek.

AYÇ 6. seviyede	**Gelişmiş siber güvenlik kavramları** - Gelişmiş siber tehditler ve saldırı vektörleri dahil olmak üzere gelişmiş siber güvenlik ilkelerini anlamak, - Siber güvenlik tehditleri ve savunma mekanizmalarındaki en son trendler hakkında farkındalık. **Siber güvenlik mevzuatı ve uyumluluk** - Ulusal ve uluslararası siber güvenlik mevzuatı, standartları ve uyumluluk gereksinimleri ve kendi sektörleriyle ilgili diğerleri hakkında bilgi.	**Gelişmiş risk değerlendirmesi ve yönetimi** - Kapsamlı risk değerlendirmeleri yapabilme - Gelişmiş metodolojileri ve araçları kullanma - Belirlenen riskleri azaltmak için etkili risk yönetimi stratejileri tasarlayın ve uygulayın. **Güvenlik mimarisi ve ağ savunmasında uzmanlık** - Güvenlik duvarları, izinsiz giriş tespit sistemleri (ids) ve izinsiz giriş önleme sistemlerinin (ips) kullanımı dahil olmak üzere güvenli ağ mimarileri tasarlayın, uygulayın ve değerlendirin. **Olay müdahalesi ve kurtarma** - Siber güvenlik olaylarına hazırlanma, müdahale etme ve kurtarma becerisi, - Kurtarma ve iş sürekliliği planları geliştirin.	**Planlama ve politika geliştirme** - Kuruluşun hedefleri ve uyumluluk yükümlülükleri ile uyumlu stratejik siber güvenlik politikaları ve çerçeveleri geliştirme ve uygulama becerisi. **Siber güvenlik girişimlerinde liderlik** - Siber güvenlik stratejilerinin uygulanmasında çalışanlara ilham verme ve rehberlik etme yeteneği de dahil olmak üzere siber güvenlik projelerine ve ekiplerine liderlik etmek ve yönetmek. **Karar verme** - Siber güvenlik uygulamalarıyla ilgili etik kararlar alın

AYÇ seviye 4/5'te olası öğrenme çıktıları şunlar olabilir:

- Öğrenciler, temel terminoloji, kimlik avı, fidye yazılımı ve DDoS saldırıları gibi siber tehdit türleri ve bunların ilgili saldırı vektörleri dahil olmak üzere siber güvenliğin temel kavramlarını öğreneceklerdir.
- Öğrenciler, potansiyel siber güvenlik risklerini ve güvenlik açıklarını belirleyebilecek, bu riskleri azaltmak için ilgili araçları ve yazılımları kullanabilecek ve güvenli parola oluşturma ve güvenli tarama gibi temel siber güvenlik uygulamalarını uygulayabilecektir.
- Öğrenciler, bir kuruluş içindeki bilgi güvenliği ve risk yönetimi için stratejiler ve politikaların yanı sıra siber güvenlik mevzuatı, standartları ve uyumluluk gereksinimleri hakkında bilgi sahibi olacaklardır.
- Öğrenciler, potansiyel güvenlik tehditlerini etkili bir şekilde değerlendirme ve azaltma yetkinliğini geliştirecek ve tehditleri ve ihlalleri uygun kanallara bildirmek de dahil olmak üzere siber güvenlik sorunlarını kuruluş içinde açık ve etkili bir şekilde iletecektir.

AYÇ 6. seviyede, olası öğrenme çıktıları şunlar olabilir:

- Öğrenciler, karmaşık siber tehditleri ve saldırı vektörlerini belirleme ve siber güvenlik savunmalarındaki en son trendler hakkında bilgi sahibi olma yeteneği de dahil olmak üzere siber güvenlik ilkeleri hakkında ileri düzeyde bir anlayış geliştireceklerdir.
- Öğrenciler, ulusal ve uluslararası siber güvenlik mevzuatı, standartları ve uyumluluk gereksinimleri hakkında kapsamlı bilgi edinecek ve bu anlayışı sektörlerinin özel ihtiyaçlarına göre uyarlayacaktır.
- Öğrenciler, gelişmiş metodolojiler ve araçlar kullanarak ve bu riskleri azaltmak için etkili risk yönetimi stratejileri oluşturarak ayrıntılı risk değerlendirmeleri yapabileceklerdir.
- Öğrenciler, güvenlik duvarları, IDS ve IPS gibi kritik güvenlik teknolojilerinin kullanımında uzmanlaşmak da dahil olmak üzere güvenli ağ mimarileri tasarlayacak, uygulayacak ve değerlendirecektir.
- Öğrenciler, olay müdahale ve kurtarma stratejilerini planlama ve yürütme, etkili kurtarma ve iş sürekliliği planları yoluyla organizasyonel esnekliği sağlama konusunda yetkin olacaklardır.
- Öğrenciler, stratejik politikalar geliştirerek, siber güvenlik projelerini ve ekiplerini yöneterek ve baskı altında bilinçli, etik kararlar alarak siber güvenlikte liderlik göstereceklerdir.

5. EKLER

5.1. EK A: İNCELENEN LITERATÜR LISTESI

Mesleki Eğitim ve Öğretim siber güvenlik eğitimine genel bakış

1. https://ccb.belgium.be/en/ict-security-education-belgium
2. https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
3. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
4. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=yüzgeç
5. http://www.anc.edu.ro/standarde-pregatire-profesionala/
6. http://217.73.164.21/index.php/articles/curriculum/c556+592/
7. http://217.73.164.21/index.php/articles/c560/
8. https://www.agerpres.ro/english/2023/09/19/first-master-s-program-in-romania-in-cyber-security-accredited-by-eit-digital-at-ubb-cluj-napoca--1171675
9. https://dnsc.ro/invatamant/vezi/5
10. https://www.linkedin.com/posts/eit-digital_ubb-cluj-joins-eit-digital-adding-cybersecurity-activity-7031990099756081152-Sr77/?originalSubdomain=si
11. https://www.unitbv.ro/documente/curriculum-syllabus/Master/Plan%20inv/MI_master_TIN_2017_2018_PI.pdf
12. https://mateinfo.unitbv.ro/images/2023/planuri_inv/Plan_inv_2023_2025_Tehnologii_moderne_in_ingineria_sistemelor_soft.pdf
13. https://drive.google.com/drive/folders/1h9aC1xwobVtGN4qNukWMvDPXICf62FgF
14. İspanya'da Siber Güvenlik Yeteneğinin Analizi ve Teşhisi, Mart 2022, Observaciber, https://www.observaciber.es/
15. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
16. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
17. Catálogos de formación en ciberseguridad, INCIBE, 2023 https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad
18. Plan Nacional de competencias digitales https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/plan-nacional-competencias-digitales.aspx
19. Plan España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
20. Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
21. Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963

Siber güvenlik zorlukları ve sektör ihtiyaçları

1. El estado de la ciberseguridad en España, Deloitte, 2022 **https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html**
2. Ferreirós Orihuel, Inés (koordinat). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) **https://digital.csic.es/handle/10261/310469**
3. El reto de la ciberseguridad en España: un país vulnerable, Telefónica https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/ **https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/**
4. Los retos de la ciberseguridad para las empresas españolas, Byte ti, 11 de enero de 2024 **https://revistabyte.es/tema-de-portada-byte-ti/retos-de-la-ciberseguridad/**
5. La falta de profesionales acentúa la amenaza de los ciberataques, el Periódico de España, 7 de Marzo de 2023 **https://www.epe.es/es/tecnologia/20230307/falta-profesionales-acentua-amenaza-ciberataques-84230209**
6. İspanya'da Siber Güvenlik Yeteneğinin Analizi ve Teşhisi, Mart 2022, Observaciber, **https://www.observaciber.es/**
7. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación **https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf**
8. Panorama actual de la Ciberseguridad en España **https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf**
9. Plan España Digital 2025 **https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx**
10. **Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf**

11. https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
12. http://data.europa.eu/esco/occupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28
13. https://nsm.no/fagomrader/digital-sikkerhet/
14. https://www.bdo.no/nb-no/nyheter/2023/na-jakter-hackerne-de-sma-selskapene
15. https://www.evelon.no/artikler/trussellandskapet-i-europa
16. https://norsis.no/sikkerhetskultur2023/sammendrag/
17. https://serit.no/hva-er-god-datasikkerhet-i-bedriften/
18. https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf

Siber güvenlikte kadınlar

1. Microsoft. (2017, Mart). Avrupa'nın kızları neden STEM eğitimi almıyor? Erişim tarihi: 20 Ocak 2024, https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf
https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf
2. Kadınlar teknolojiye gidiyor (2021, Eylül). Avrupa'da BİT işgücü ve Covid-19 sonrası toplumsal cinsiyet sorunu. Women Go Tech. Erişim tarihi: 20 Ocak 2024, https://womengotech.com/app/uploads/2021/09/ICT-workforce-in-Europe-and-its-gender-challenge.pdf
3. Rodiklių duomenų bazė - Oficialiosios statistikos portalas. (tarih yok) 1. https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/
4. Bukauskas, Brilingaite, Ikamas, Juozapavicius ve Lepaite. (2022, 5 Ağustos). Ataskaita Lietuvos kibernetinio saugumo kompetencijų žemelapis. Vilnius Üniversitesi. Erişim tarihi: 20 Ocak 2024, https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf
5. https://www.digi.no/artikler/debatt-flere-tech-jenter-ma-til-for-a-finne-morgendagens-losninger/535073
6. https://odanettverk.no/2022/03/08/dette-er-norges-50-fremste-tech-kvinner-2022/
7. https://e24.no/naeringsliv/i/k6Goma/etterlyser-flere-kvinner-til-cybersikkerhet
8. https://www.ssb.no/befolkning/artikler-og-publikasjoner/kvinner-velger-fortsatt-kvinneyrker
9. https://live.worldbank.org/en/event/2023/women-business-law-2023
10. https://wbl.worldbank.org/en/data/exploreeconomies/romania/2023
11. https://eige.europa.eu/gender-equality-index/2022/country/RO
12. https://cybernews.com/editorial/cyber-women-grim-statistics-big-opportunities/
13. https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/
14. https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-winFerreirós Orihuel, Inés (koordinat). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) https://fundacionalternativas.org/publicaciones/iv-informe-sobre-la-ciencia-y-la-tecnologia-en-espana/
15. Mujeres empleadas en ciencia y tecnología (reparto por sectores). İspanya, UE-27 ve UE-28. Seri 2019-2021. https://www.ine.es/jaxi/Tabla.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c02002.px&L=0
16. La mujer en la ciencia española, en datos y gráficos, EpData, 7 de marzo de 2023 https://www.epdata.es/datos/mujer-ciencia-espanola-datos-estadisticas/298
17. İspanya'da Siber Güvenlik Yeteneklerinin Analizi ve Teşhisi, Mart 2022, Observaciber, https://www.incibe.es/ed2026/talento-hacker/publicaciones/diagnostico-talento-ciberseguridad
18. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
19. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

5.2. EK B: ANKET ANKETI

Mesleki Eğitim ve Öğretim anketi

Bu anket, siber güvenlik eğitiminin mevcut durumu ve gelecekteki ihtiyaçları hakkında bilgi toplamak ve Küçük ve Orta Ölçekli İşletmeler (KOBİ'ler) için siber güvenlik zorluklarına göre uyarlanmış etkili bir siber güvenlik eğitim programının şekillendirilmesine yardımcı olmak için tasarlanmıştır.

Anket 4 bölüme ayrılmıştır:

- Demografik
- Müfredat, eğitim ihtiyaçları ve öğrenme tercihleri
- Yetkinlik gereksinimleri ve gelecekteki beceriler
- Cinsiyete özel içgörüler

Anketin tamamlanması yaklaşık 8 dakika sürecektir.

DEMOGRAFİK

Ülkeniz neresi?
▫ Litvanya
▫ Belçika
▫ Norveç
▫ Türkiye
▫ Finlandiya
▫ Romanya
▫ İspanya
▫ Polonya

Şu anda hangi okul kurumunda öğretmenlik yapıyorsunuz?
▫ VET (Mesleki Eğitim ve Öğretim)
▫ HEI (Yüksek Öğrenim (HE) kurumu)

Cinsiyetiniz nedir?
▫ Erkek
▫ Kadın
▫ Söylememeyi tercih ederim

Kaç yıldır siber güvenlik eğitimine katılıyorsunuz?
▫ 1 yıldan az
▫ 1-5 yıl
▫ 6-10 yıl
▫ 10 yıldan fazla

MÜFREDAT, EĞİTİM İHTİYAÇLARI VE ÖĞRENME TERCİHLERİ

Siber güvenlik eğitim programınızda aşağıdaki konulardan hangileri yer alıyor? (Uygun olanların tümünü seçin)
▫ Siber Güvenliğin Temelleri

▫ Tehdit Analizi ve Yönetimi
▫ Gelişmiş tehdit azaltma teknikleri
▫ Kriptografisi
▫ Ağ Güvenliği
▫ Siber Güvenlik Yasaları ve Politikaları
▫ Risk Yönetimi
▫ Olay Müdahalesi
▫ Diğer: _____

Siber güvenlik eğitiminizde öncelikli olarak hangi öğretim yöntemlerini kullanıyorsunuz? (Uygun olanların tümünü seçin)

▫ Dersleri
▫ Uygulamalı Laboratuvarlar
▫ Örnek Olay İncelemeleri
▫ Grubu Projeleri
▫ Çevrimiçi Simülasyonlar
▫ Ters Yüz Sınıf

Başka:_____

Siber güvenlik eğitimi için en etkili öğrenme biçimleri hangileridir? (Uygun olanların tümünü seçin)

▫ Yüz yüze atölye çalışmaları
▫ Çevrimiçi kurslar
▫ Web Seminerleri
▫ Etkileşimli animasyonlar
▫ Video eğitimleri
▫ Uygulamalı uygulama oturumları
▫ Diğer: _____

Etkili siber güvenlik eğitimi verirken karşılaştığınız en büyük zorluklar nelerdir?

Açık soru

1'den 5'e kadar bir ölçekte, mevcut eğitim programlarının öğrencileri gerçek dünyadaki KOBİ'lerin siber güvenlik zorluklarına ne kadar etkili bir şekilde hazırladığını düşünüyorsunuz?

▫ Çok Etkisiz
▫ Biraz Etkisiz
▫ Nötr
▫ Biraz Etkili
▫ Çok Etkili

Mevcut siber güvenlik eğitiminin KOBİ'lerin özel ihtiyaçlarıyla ne kadar uyumlu olduğuna inanıyorsunuz?

1 (Hizalanmamış)
2 (Hafifçe hizalanmış)
3 (Hizalanmış)
4 (İyi hizalanmış)
5 (Yüksek hizalı)

KOBİ'lerin benzersiz siber güvenlik ihtiyaçlarını karşılamak için eğitiminize dahil ettiğiniz belirli konular veya beceriler var mı? (Uygun olanların tümünü seçin)

▫ KOBİ'ler için Temel Siber Güvenlik
▫ KOBİ Bağlamında Risk Değerlendirmesi ve Yönetimi
KOBİ'ler için ▫ Olay Müdahalesi
▫ KOBİ'ler için Veri Koruma ve Gizlilik
▫ KOBİ'ler için Siber Güvenlik Politikası Geliştirme
▫ Diğer: _____

KOBİ'lere daha iyi hizmet vermek için siber güvenlik eğitiminizi ne sıklıkla özelleştiriyor veya uyarlıyorsunuz?

▫ Her zaman
▫ Sık
▫ Bazen
▫ Nadiren
▫ Asla

Geri bildirim alıyor musunuz veya eğitim içeriğinizin onların ihtiyaçlarına uygunluğunu sağlamak için KOBİ temsilcileri veya profesyonelleri ile iletişim halinde misiniz?

▫ Evet, düzenli olarak
▫ Ara sıra
▫ Nadiren
▫ Asla

Deneyimlerinize dayanarak, mevcut siber güvenlik eğitiminin KOBİ profesyonellerini siber güvenlik zorluklarıyla başa çıkacak şekilde donatmada ne kadar etkili olduğuna inanıyorsunuz?

▫ Çok Etkisiz
▫ Biraz Etkisiz
▫ Nötr
▫ Biraz Etkili
▫ Çok Etkili

KOBİ'ler için siber güvenlik eğitiminin uygunluğunu ve etkinliğini artırmak için ne gibi önerileriniz var?

Açık soru

YETKINLIK GEREKSINIMLERI VE GELECEKTEKI BECERILER

Sizce, mevcut KOBİ siber güvenlik işgücündeki en önemli beceri eksiklikleri nelerdir? (En fazla üç tane seçin)

▫ Tehdit algılama ve müdahale
▫ Bulut güvenliği uzmanlığı
▫ Uyumluluk ve mevzuat bilgisi
▫ Olay müdahalesi ve kurtarma
▫ Risk yönetimi ve analizi
▫ Veri gizliliği ve koruması

▫ Gelişen teknolojiler
▫ Ağ güvenliği

Lütfen yetkinlikleri ve bilgi ihtiyaçlarını 1 (gerekli değil) ile 5 (çok gerekli) arasında bir ölçekten derecelendirin:

	Derecelendirme				
Risk Değerlendirmesi ve Yönetimi Risk türlerini ve etkilerini anlamak.					
Teknik Bilgi Siber güvenliğin teknik yönleri ve işletim sistemleri, ağ iletişimi ve veritabanı yönetimi bilgisi.					
Olay Müdahalesi ve Kurtarma Güvenlik ihlallerini ve olaylarını belirleme, bunlara yanıt verme ve bunlardan kurtarma.					
Politika Geliştirme ve Uygulama Etkili güvenlik politikaları ve uygulamaları geliştirmek ve uygulamak.					
Tehdit İstihbaratı ve İzleme En son siber güvenlik trendleri, tehditler ve saldırı metodolojileri ile güncel kalmak.					
İletişim Becerileri Siber güvenlik konularında personel, yönetim ve muhtemelen müşterilerle etkili iletişim.					
Veri Gizliliği ve Koruması Veri gizliliği ilkeleri ve hassas bilgilerin nasıl korunacağı.					

KOBİ'ler için son derece ihtiyaç duyulabilecek önceki soruda listelenmeyen herhangi bir ilgili beceri ve bilgi seti görüyor musunuz?
Açık soru
Önümüzdeki 5 yıl içinde KOBİ'lerin hangi siber güvenlik tehditlerine karşı hazırlıklı olması gerektiğini düşünüyorsunuz? (En fazla üç tane seçin)
▫ Ransomware saldırıları
▫ IoT güvenlik açıkları
▫ Bulut güvenlik ihlalleri
▫ Yapay zeka güdümlü siber saldırılar
▫ İçeriden gelen tehditler
▫ Diğer: _____
Önümüzdeki 5 yıl için siber güvenlik eğitiminde öne çıkan ilk 3 trend olarak neler öngörüyorsunuz? (En fazla 3 seçenek belirleyin)
▫ Siber Güvenlikte Yapay Zeka ve Makine Öğrenimi
▫ Sosyal becerilere ve disiplinler arası eğitime odaklanın
▫ Kuantum Bilişim Tehditleri
▫ Etik Hacking ve Savunma Becerileri

▫ Dijital Kimlik ve Gizlilik
▫ Merkezi olmayan güvenlik sistemleri (ör. Blockchain)
▫ Diğer: _____

Siber güvenlik eğitimi için son derece etkili olduğuna inandığınız belirli eğitim yöntemleri, araçları veya platformları var mı?
Metni aç
KOBİ'ler için siber güvenlik eğitimini iyileştirmeye yönelik başka yorumlarınız veya önerileriniz var mı?
Metni aç

CINSIYETE ÖZEL IÇGÖRÜLER
Siber güvenlik eğitim programlarınıza katılanlar arasında tahmini kadın yüzdesi nedir?
▫ %10'dan az
▫ %10 - %25
▫ %26 - %50
▫ %51 - %75
▫ %75'ten fazla
Kadınların siber güvenlik eğitimine katılımını teşvik etmek için uyguladığınız belirli girişimler veya stratejiler var mı?
▫ Evet
▫ Hayır
Cevabınız evet ise, lütfen belirtin: _____
Siber güvenlik alanında yeterli sayıda toplumsal cinsiyet kapsayıcı eğitim modülü olduğuna inanıyor musunuz?
▫ Evet
▫ Hayır
▫ Emin değilim
▫ Benimle alakalı değil
Deneyimlerinize göre, kadınların siber güvenlik eğitimine ve kariyerlerine katılmalarını veya ilerlemelerini engelleyen başlıca engeller nelerdir? (Uygun olanların tümünü seçin)
▫ Siber güvenlikteki fırsatlar hakkında farkındalık eksikliği
▫ Stereotipler veya kültürel normlar
▫ Mentorluk veya rol model eksikliği
▫ İş-yaşam dengesi zorlukları
▫ Sektörde algılanan cinsiyet yanlılığı
▫ Diğer: _____
Kurumunuzun siber güvenlik eğitimlerinde özellikle kadınlar için çeşitliliği ve kapsayıcılığı teşvik etmek için özel politikaları veya programları var mı?
▫ Evet
▫ Hayır
▫ Emin değilim

Siber güvenlik eğitimini daha toplumsal cinsiyet kapsayıcı hale ne getirebilir? (En fazla üç tane seçin)

▫ Daha fazla kadın siber güvenlik eğitmeni veya eğitim personeli
▫ Burs veya teşvik sunun
▫ Cinsiyet önyargılarından kaçınan eğitim içeriği
▫ Başarılı kadın siber güvenlik uzmanlarının görünürlüğünün artması
▫ Kadınlara özel daha fazla eğitim seansı
▫ Toplumsal cinsiyet kapsayıcı vaka çalışmaları ve senaryolar
▫ Kişiye özel eğitim programları
▫ Mentorluk fırsatları
▫ Diğerleri: _____

KOBİ ANKETİ

Bu anket, KOBİ Siber Güvenlik Değişim Ajanları için eğitim ihtiyaçlarını haritalamayı amaçlamaktadır. Yanıtlarınız, çeşitli KOBİ'lerdeki siber güvenlik bilgi ve becerilerinin mevcut ortamını anlamaya, siber güvenlik eğitimindeki boşlukları belirlemeye ve gelecekteki eğitim programlarının etkinliğini artırmaya yardımcı olacaktır.

Anket 3 bölüme ayrılmıştır:

- Demografik
- Eğitim ihtiyaçları
- Siber güvenlikte kapsayıcılık ve kadınların ihtiyacı.

Anketin tamamlanması yaklaşık 5 dakika sürecektir.

DEMOGRAFİK

Ülkeniz neresi?

▫ Litvanya
▫ Belçika
▫ Norveç
▫ Türkiye
▫ Finlandiya
▫ Romanya
▫ İspanya
▫ Polonya

Şirketteki mevcut pozisyonunuz ve departmanınız nedir?

Konum:_____
Bölüm:_____

Cinsiyetiniz nedir?

▫ Erkek
▫ Kadın
▫ Söylememeyi tercih ederim

Şirkette kaç kişi çalışıyor?

10 çalışana kadar ▫
▫ 11-50
▫ 51-250

Çalışanların mevcut siber güvenlik bilgi ve beceri düzeyini nasıl değerlendirirsiniz?

▫ Başlangıç

▫ Orta Seviye
▫ Gelişmiş

Siber güvenlikle ilgili işleri kaç kişi gerçekleştiriyor?
Numara girin: _____

Siber güvenlik çalışmaları için harici hizmetler mi kiralıyorsunuz?
▫ Evet
▫ Hayır

EĞİTİM İHTİYAÇLARI

1 (etkisiz) ile 5 (çok etkili) arasında bir ölçekte, mevcut eğitim programlarının öğrencileri gerçek dünyadaki KOBİ'lerin siber güvenlik zorluklarına ne kadar etkili bir şekilde hazırladığını düşünüyorsunuz?
1- Etkisiz
5- Çok Etkili

Sizce, mevcut KOBİ siber güvenlik işgücündeki en önemli beceri eksiklikleri nelerdir? (En fazla üç tane seçin)
▫ Tehdit algılama ve müdahale
▫ Bulut güvenliği uzmanlığı
▫ Uyumluluk ve mevzuat bilgisi
▫ Olay müdahalesi ve kurtarma
▫ Risk yönetimi ve analizi
▫ Veri gizliliği ve koruması
▫ Gelişen teknolojiler
▫ Ağ güvenliği
▫ Diğer: _____

Lütfen yetkinlikleri ve bilgi ihtiyaçlarını 1 (gerekli değil) ile 5 (temel) arasında bir ölçekten derecelendirin:

	Derecelendirme				
Risk Değerlendirmesi ve Yönetimi Risk türlerini ve etkilerini anlamak.					
Teknik Bilgi Siber güvenliğin teknik yönleri ve işletim sistemleri, ağ iletişimi ve veritabanı yönetimi bilgisi.					
Olay Müdahalesi ve Kurtarma Güvenlik ihlallerini ve olaylarını belirleme, bunlara yanıt verme ve bunlardan kurtarma.					
Politika Geliştirme ve Uygulama Etkili güvenlik politikaları ve uygulamaları geliştirmek ve uygulamak.					
Tehdit İstihbaratı ve İzleme En son siber güvenlik trendleri, tehditler ve saldırı metodolojileri ile güncel kalmak.					
İletişim Becerileri Siber güvenlik konularında personel, yönetim ve muhtemelen müşterilerle etkili iletişim.					
Veri Gizliliği ve Koruması Veri gizliliği ilkeleri ve hassas bilgilerin nasıl korunacağı.					

KOBİ'ler için son derece ihtiyaç duyulabilecek önceki soruda listelenmeyen herhangi bir ilgili beceri ve bilgi seti görüyor musunuz?
Açık soru

Önümüzdeki 5 yıl içinde KOBİ'lerin hangi siber güvenlik tehditlerine karşı hazırlıklı olması gerektiğini düşünüyorsunuz? (En fazla üç tane seçin)
▫ Ransomware saldırıları

▫ IoT güvenlik açıkları
▫ Bulut güvenlik ihlalleri
▫ Yapay zeka güdümlü siber saldırılar
▫ İçeriden gelen tehditler
▫ Diğer: _____

Varsa, çalışanın mevcut siber güvenlik bilgi veya beceri durumunda hangi belirli boşlukların olduğunu düşünüyorsunuz?
▫ Düşük seviyede Teknik beceri
▫ Düşük düzeyde Sosyal beceriler
▫ Düşük düzeyde Güvenlik Açığı değerlendirmesi
▫ Düşük düzeyde Politika ve yönetmelik anlayışı
▫ Düşük düzeyde Tehdit farkındalığı
▫ Düşük seviyede Siber Güvenlik düzenli eğitimleri
▫ Diğer: _____
Önümüzdeki 5 yıl için siber güvenlik eğitiminde öne çıkan ilk 3 trend olarak neler ön-görüyorsunuz? (En fazla 3 seçenek belirleyin)
▫ Siber Güvenlikte Yapay Zeka ve Makine Öğrenimi
▫ Sosyal becerilere ve disiplinler arası eğitime odaklanın
▫ Kuantum Bilişim Tehditleri
▫ Etik Hacking ve Savunma Becerileri
▫ Dijital Kimlik ve Gizlilik
▫ Merkezi olmayan güvenlik sistemleri (ör. Blockchain)
▫ Diğer: _____

SIBER GÜVENLIKTE KAPSAYICILIK VE KADINLARIN IHTIYAÇLARI
Mevcut siber güvenlik eğitiminin kapsayıcı olduğunu ve tüm cinsiyetlerin ihtiyaçlarını etkili bir şekilde ele aldığını düşünüyor musunuz?
▫ Evet
▫ Hayır
▫ Emin değilim
Kendinizi kadın olarak tanımlıyorsanız, siber güvenlik eğitimlerine/çalışmalarına erişimde veya bunlara katılmada herhangi bir engel veya zorlukla karşılaştınız mı?
▫ Evet
▫ Hayır
▫ Söylememeyi tercih ederim
▫ Evet ise, lütfen belirtin: _____
Kuruluşunuzda kadınların siber güvenliğe katılımını özel olarak destekleyen veya teşvik eden herhangi bir girişim veya programdan haberdar mısınız?
▫ Evet
▫ Hayır
▫ Emin değilim
Kuruluşunuzda daha fazla kadını siber güvenlik eğitimine katılmaya teşvik edecek destek veya kaynak türleri nelerdir? (Açık uçlu)
Açık soru
Siber güvenlik eğitiminin etkinliğini artırmak için ne gibi iyileştirmeler veya yenilikler önerirsiniz?
Açık soru

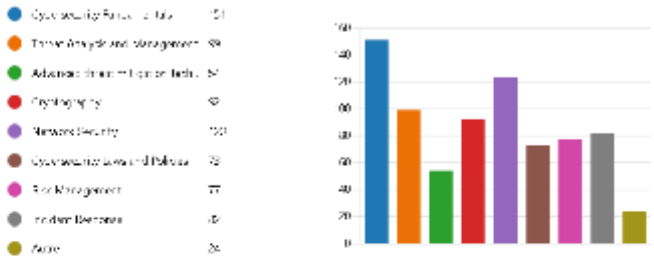
5.3. EK C: ANKET SONUÇLARI

Mesleki Eğitim ve Öğretim

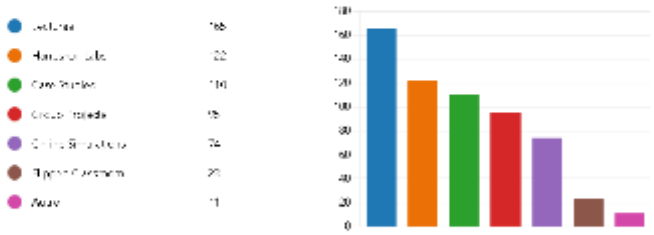
Mapping the training needs for SME Cyber Security Change Agents - VET and HEI survey

190 Responses

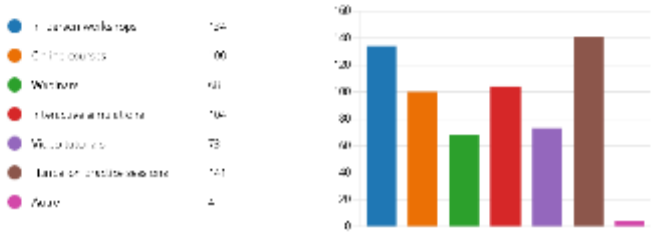
1. Which of the following topics are included in your cybersecurity training program? (Select all that apply)



2. What teaching methods do you primarily use in your cybersecurity training? (Select all that apply)



3. What teaching method would be the most effective for cybersecurity training? (Select all that apply)



4. **What are the biggest challenges you face in delivering effective cybersecurity training?**

190
Réponses

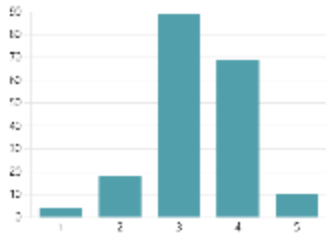
Dernières réponses
-
-
keeping up with Technology Changes, Basic knowledge of the students, Soft...

Mettre à jour

34 répondants (17.9 %) répondu students pour cette question

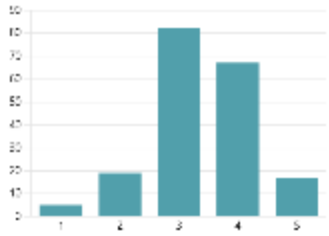
5. **On a scale of 1 (Very Ineffective) to 5 (Very Effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.33
Évalué en moyenne

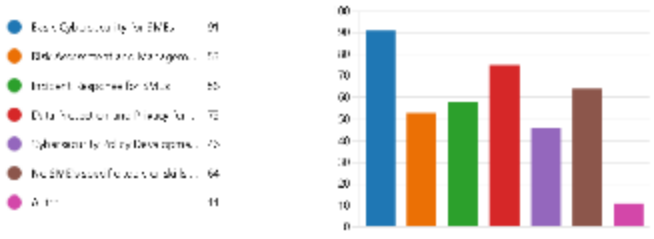


6. **On a scale of 1 (Not aligned) to 5 (Highly aligned), how well do you believe the current cybersecurity training aligns with the specific needs of SMEs?**

3.38
Évalué en moyenne



7. **Are there specific topics or skills that you include in your training to address the unique cybersecurity needs of SMEs? (Select all that apply)**



8. **How often do you customize or adapt your cybersecurity training to better cater to SMEs?**

9. **Do you receive feedback or are you in contact with SME representatives or professionals to ensure the relevancy of your training content to their needs?**

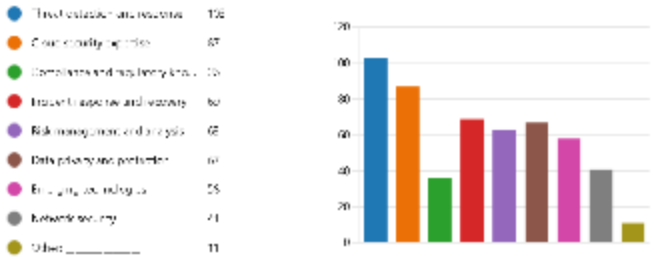
10. **Based on your experience, how effective do you believe the current cybersecurity training is in equipping SME professionals to handle cybersecurity challenges?**

11. **What suggestions do you have for improving the relevance and effectiveness of cybersecurity training for SMEs?**

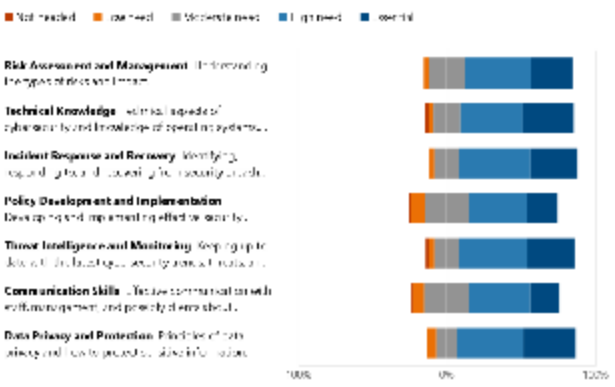
117
Réponses

Dernières réponses

12. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



13. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



14. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

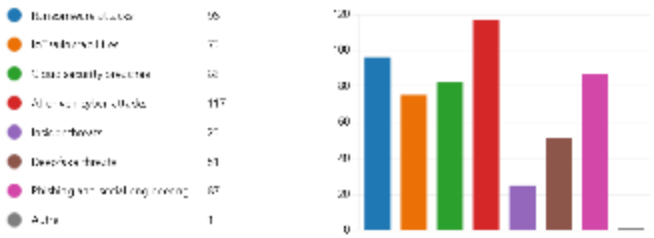
190
Réponses

Dernières réponses
-"
-"
"Cloud Security AI"

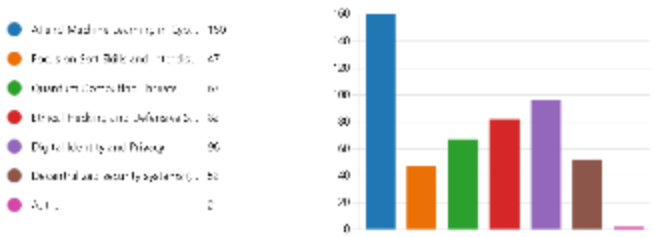
Mettre à jour

10 répondants (5%) répondu skills pour cette question.

15. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. Are there any particular training methods, tools, or platforms that you believe are exceptionally effective for cybersecurity education?

115
Réponses

Dernières réponses

18. Any additional comments or suggestions for improving cybersecurity training for SMEs?

80
Réponses

Dernières réponses

19. What is the estimated percentage of women among the participants in your cybersecurity training programs?

20. Are there any specific initiatives or strategies you employ to encourage women's participation in cybersecurity training?

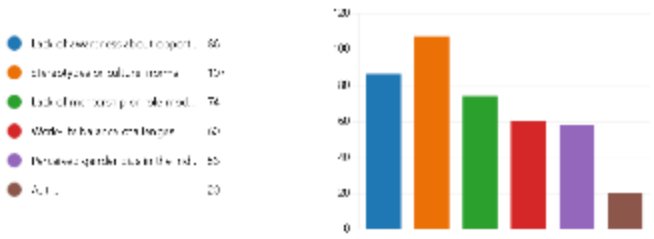
21. If you replied "Yes" to the previous question, please specify

35
Réponses

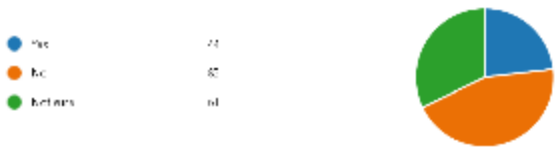
Dernières réponses

22. Do you believe there are enough gender-inclusive training modules available in cybersecurity?

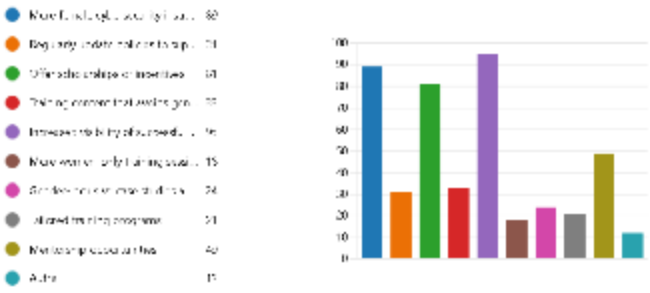
23. In your experience, what are the primary barriers that prevent women from participating or advancing in cybersecurity training and careers? (Select all that apply)



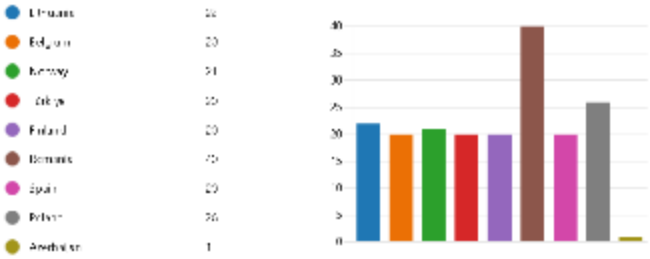
24. Does your institution have specific policies or programs to promote diversity and inclusion, particularly for women, in cybersecurity training?



25. What could make cybersecurity training more gender-inclusive? (Choose up to three)

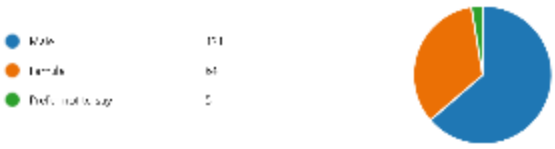


26. What is your country?

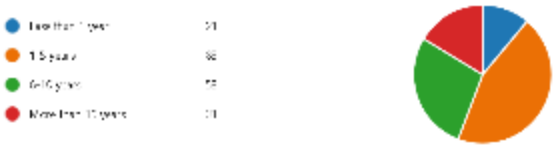


27. In which school institution are you currently teaching?

28. What is your gender?



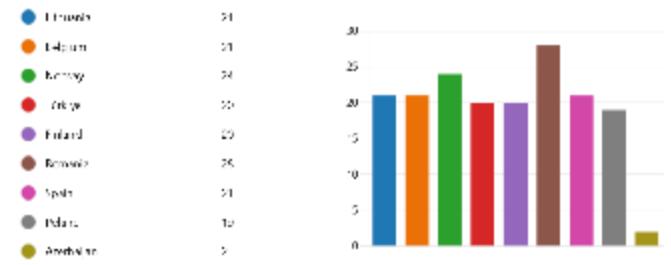
29. How many years have you been involved in cybersecurity training? (Either general, specific, short and long trainings)



Mapping the training needs for SME Cyber Security Change Agents - SMEs survey

176 Responses

1. What is your country?



2. What is your company sector?

176
Réponses

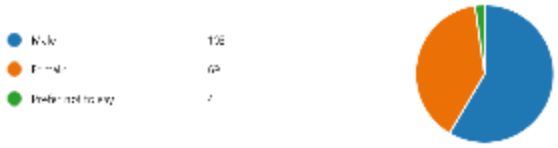
3. What is your current position in the company?

176
Réponses

Dernières réponses

Mettre à jour

4. What is your gender?



5. How many employees are working in the company?

6. How would you rate employees' current level of cybersecurity knowledge and skills?

7. How many employees perform work related to cybersecurity?

176
Réponses

Dernières réponses

Mettre à jour

responsible/manager
non
n't have that information
information
people
~100
13
100
1
none
50
2
20
110
30
5
lot of lectures
No idea
staff members
trainers- practicer

8. How many of these employees are women?

176
Réponses

Dernières réponses

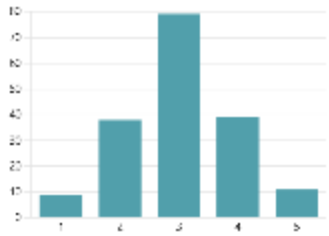
Mettre à jour

n't have that information
sales rep
men
One
10
7
1
5
11
12
non
information
2
6
No idea
none
4
max
persons
woman for sure

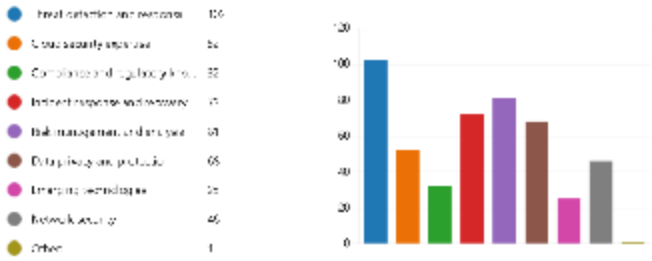
9. Do you hire external services for cybersecurity work?

10. On a scale of 1 (ineffective) to 5 (very effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?

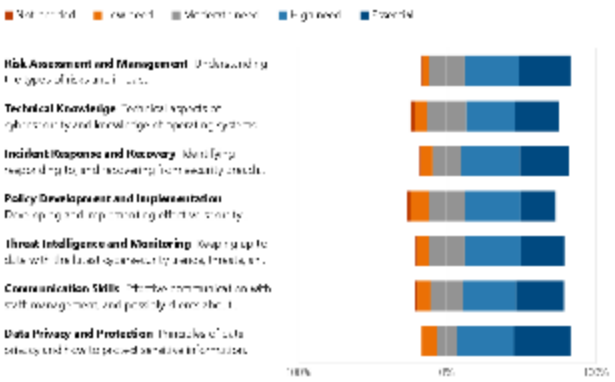
3.03
Évaluation moyenne



11. In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)



12. Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:



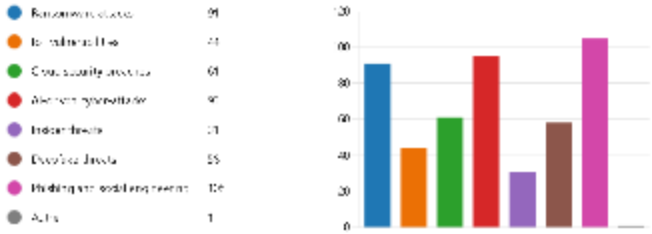
13. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

175
Réponses

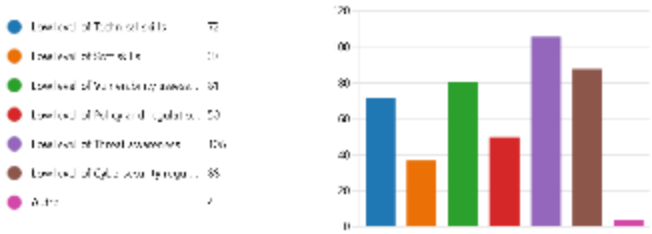
Dernières réponses
We assume it is not subject matter experts (SMEs) in a big company are ...
Cyber Security on all these topics around Generative AI - which is complete...
Not sure

4 répondants (2 %) n'ont répondu skills pour cette question

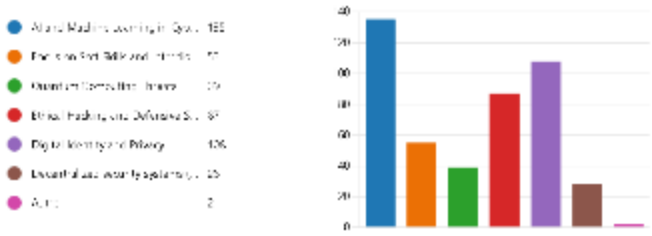
14. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



15. **What specific gaps, if any, do you feel exist in employee's current cybersecurity knowledge or skills status? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. Do you feel that current cybersecurity training is inclusive and addresses the needs of all genders effectively?

18. If you identify as female, have you faced any barriers or challenges in accessing or participating in cybersecurity training/studies?

19. If you replied "Yes" to the previous question, please specify

11
Reponses

Dernières réponses

20. Are you aware of any initiatives or programs within your organization that specifically support or promote the participation of women in cybersecurity?

21. If you replied "Yes" to the previous question, please specify

17
Réponses

Dernières réponses

5.4. EK D: İNCELENEN ESCO MESLEKLERININ LISTESI

Başvuru:
2529.1 https://esco.ec.europa.eu/sites/default/files/chief%20ICT%20security%20officer.pdf
2529.2 https://esco.ec.europa.eu/sites/default/files/digital%20forensics%20expert.pdf
2529.3
https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F1c5a896a-e010-4217-a29a-c44db26e25da
2529.4 https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
2529,5 https://esco.ec.europa.eu/sites/default/files/ICT%20resilience%20manager.pdf
2529,6 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20administrator.pdf
2529,7 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20consultant.pdf
2529.8 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20manager.pdf
2529,9 https://esco.ec.europa.eu/sites/default/files/knowledge%20engineer.pdf

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau