CyberAgent

Co-funded by the European Union

KOBİ'LER IÇIN İYI UYGULAMALAR REHBERI

SIBER AJAN 06.2026

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.

www.cyberagents.eu

Çalışma Paketi 6: Yayım ve Sömürü

Teslimat 6.4: KOBİ'ler için İyi Uygulamalar Rehberi

WP6 Lideri – Women4Cyber Vakfı

İÇERİKTE

TABLO LISTESI

GIRIŞ

CyberAgent projesi, Romanya, Belçika, Norveç, İspanya, Türkiye, Polonya, Litvanya ve Finlandiya olmak üzere sekiz Avrupa ülkesinde üç yıl boyunca geliştirildi. CyberAgent, KOBİ çalışanları, VET öğrencileri ve yükseköğretim öğrencileri için modüler, erişilebilir bir siber güvenlik eğitim programı oluşturmak ve test etmek amacıyla oluşturuldu. Bu çalışmanın temel sonucu, Siber Güvenlik Değişim Ajanıdır: eğitimli, uzman olmayan bir çalışan ve kuruluşlarında siber güvenlik farkındalığı için iç referans noktası olarak görev yapar.

Bu Rehber, projenin uygulama deneyimini KOBİ'ler için pratik rehberliğe dönüştürür. Değişim Ajanı rolünün ne olduğunu, doğru kişiyi nasıl belirleyip atayacağını, eğitimini nasıl destekleyeceğini ve cinsiyet kapsayımının sürecin başından itibaren nasıl entegre edileceğini açıklıyor. Sonunda bir kontrol listesi, KOBİ'lerin her aşamada doğru koşulların sağlandığını doğrulamasına yardımcı olur.

1. SIBER GÜVENLIK HER KOBİ IÇIN NEDEN ÖNEMLIDIR?

ENISA Threat Landscape 2025 raporuna göre, siber suçlular saldırılarını sanayileştiriyor ve KOBİ'leri büyüklükleri ve sektörleri ne olursa olsun yüksek değerli hedefler haline getiriyor. Bugün kuruluşların karşılaştığı en yaygın tehditler fidye yazılımı, oltalama ve veri ihlalleridir. Fidye yazılımı ve veri ihlalleri, AB kuruluşlarını hedef alan siber suç olaylarının çoğunluğunu oluşturuyor; suçların %80'inden fazlasını fidye yazılımı oluşturuyor. Bu saldırıların sanayileşmesi, özellikle "Hizmet olarak Fidye Yazılımı" modeli, saldırganlar için engelleri azalttı ve en küçük kuruluşları bile hedefe dönüştürdü.

Özellikle KOBİ'ler için, bir siber saldırının sonuçları sadece geçici kesintilerle sınırlı değildir. ENISA'ya göre, siber güvenlik saldırıları bir hafta sonra KOBİ'lerin %90'ının işletmeleri üzerinde ciddi olumsuz etkiler yaratıyor. Ancak, bu maruzeye rağmen, KOBİ'lerin nadiren özel BT veya güvenlik personeli vardır ve çalışanları nadiren yapılandırılmış siber güvenlik eğitimi alır. Avrupa'daki KOBİ'ler yaklaşık 100 milyon kişiyi istihdam ediyor ve Avrupa'nın GSYİH'sının yarısından fazlasını oluşturuyor. Bu nedenle, KOBİ sektöründeki siber güvenlik açığı ekonomik ve toplumsal bir risktir.

Çoğu siber saldırı, bir oltalama bağlantısına tıklama, zayıf şifreler veya doğrulanmamış e-postalar gibi insan faktörleri sayesinde başarılı olur. Bu, ilk savunma hattının teknik bir araç olmadığı, neye dikkat edilmesi gerektiğini ve bir şeyler ters gittiğinde ne yapması gerektiğini bilen bilgili ve bilinçli bir çalışan olduğu anlamına gelir. Bu rol tam olarak Siber Güvenlik Değişim Ajanı tarafından kapsanıyor.

2. SIBER GÜVENLIK DEĞIŞIM AJANI

Siber Güvenlik Değişim Ajanı kavramı, CyberAgent projesinin kalbinde yer alır. Bu bölüm, rolün ne olduğunu, neden geliştirildiğini ve Küçük ve Orta Ölçekli İşletmeler (KOBİ) içinde pratikte nasıl göründüğünü açıklar.

2.1. NEDIR VE NEDEN GEREKLI

KOBİ'ler Avrupa ekonomisinin belkemiğidir, ancak siber güvenlik tehditlerine en çok maruz kalan kuruluşlar arasında kalmaya devam ediyorlar. Büyük şirketlerin aksine, çoğu KOBİ'nin özel BT veya güvenlik departmanları yoktur ve çalışanları nadiren yapılandırılmış siber güvenlik eğitimi alır. Bu durum, KOBİ'lerin karşılaştığı siber riskler ile bunlarla başa çıkma kapasitesi arasında kalıcı bir boşluk yaratıyor.

CyberAgent projesi ve Siber Güvenlik Değişim Ajanı figürleri, mevcut ekipler içinde farklı bir yetenek oluşturarak bu boşluğu kapatmak için tasarlandı. Siber Güvenlik Değişim Ajanı, eğitimli, teknik olmayan bir çalışandır ve siber güvenlik farkındalığı için iç referans olarak görev yapar, daha güvenli davranışları teşvik eder, yaygın riskleri tanır ve kuruluş içinde daha iyi siber güvenlik uygulamalarını uygular. Bu rakam ayrıca olaylar durumunda meslektaşlar için uygun destek konusunda bir rehber olarak hizmet verecektir.

Bu role olan gereklilik, CyberAgent pilotu boyunca toplanan kanıtlarla doğrulanmaktadır. Sekiz ortak ülkede eğitim, KOBİ çalışanları, yükseköğretim ve mesleki eğitimi alanlar arasında 594 kayıtlı katılımcıya ulaştı. KOBİ çalışanları, genellikle zaman kısıtlamaları ve iş sorumlulukları nedeniyle eğitim ortamlarında ulaşılması ve elde tutulması en zor hedef grup olarak tanımlanır. Buna rağmen, KOBİ çalışanları arasındaki yüksek tamamlama oranı, günlük işlerde siber güvenlik farkındalığının gerçek önemini yansıtmaktadır.

2.2. TEMEL SORUMLULUKLAR

Siber Güvenlik Değişim Ajanı, siber güvenlik sorunlarını tek başına çözmekten sorumlu değildir. Rol, farkındalık, iletişim ve koordinasyon etrafında inşa ediliyor; siber güvenliği gündemde tutan ve meslektaşlarının günlük işlerinde bu konuda yol almasına yardımcı olan kişi olmak üzere. Bunların hiçbiri teknik uzmanlık gerektirmez. Bunun gerektirdiği, kurum içinde güvenilir biri, iyi bağlantıları olan ve siber güvenliği ekibin çalışma şeklinin normal bir parçası haline getirmeye motive olmuş biri.

Somut olarak, bu rol önemli bir zaman gerektirmeyen ancak organizasyonun güvenlik kültürü üzerinde anlamlı bir etkisi olan tekrarlayan hafif faaliyetler setine dönüşür:

- **Düzenli olarak farkındalık** yaratmak. Change Agent, oltalama e-postaları, zayıf şifreler, güvensiz veri işleme, şüpheli bağlantılar gibi en yaygın tehditler hakkında meslektaşlarıyla düzenli olarak farkındalık mesajları paylaşıyor; bu durum bir yük haline gelmeden siber güvenliğin görünür olmasını sağlıyor. Bu, ekip sohbetinde aylık paylaşılan bir mesaj, yoğun bir dönem öncesi kısa bir hatırlatma veya sektörde dolaşan yeni bir dolandırıcılık türü hakkında bir not kadar basit olabilir. Format tutarlılıktan daha az önemli.

- **Siber güvenliği toplantı gündeminde tutmak**. Change Agent, takım toplantılarında kısa ve pratik tartışmalarla siber güvenlik konularını gündeme getirir. Bu, uzun sunumlar veya resmi eğitim oturumları anlamına gelmez. Son zamanlarda gerçekleşen bir oltalama girişimi hakkında beş dakikalık bir sohbet veya şifrelerin güncellenmesiyle ilgili bir hatırlatma, farkındalığı canlı tutmak ve siber güvenliğin ortak bir organizasyon sorumluluğu olduğunu, teknik personele devredilmediğini göstermek için yeterlidir.

- **Olay raporlamalarını teşvik** ediyor. Siber Güvenlik Değişim Ajanı'nın en önemli katkılarından biri, çalışanların alışılmadık bir e-posta, beklenmedik davranan bir sistem, bir meslektaşının olmaması gereken bir şeye tıklaması gibi şüpheli durumları bildirmekten rahatça hissettikleri bir kültür yaratmaktır. Birçok siber güvenlik olayı, çalışanların utanç veya suçlama korkusuyla erken uyarı işaretlerini bildirmemesi nedeniyle büyür. Change Agent, yaklaşılabilir ve süreç hakkında net bir şekilde raporlamayı normalleştirmeye yardımcı olur.

- **Onboarding'i destekliyor**. Yeni çalışanlar, siber güvenlik açısından herhangi bir kuruluşun en savunmasız üyeleri arasındadır; çünkü iç prosedürlere aşina olmamaları, beklenmedik taleplere daha çok güvenmeleri ve genellikle temel güvenlik uygulamaları konusunda henüz eğitim almadıkları için. Change Agent, işe başlama sırasında siber güvenlik temellerini tanıtmada önemli bir rol oynar; iyi alışkanlıkların ilk günden itibaren oluşturulmasını sağlar; sonradan yenilenmek yerine iyi alışkanlıklar elde edilir.

- **İçsel bir temas noktası olarak hareket** ediyor. Siber Güvenlik Değişim Ajanı, meslektaşların siber güvenlik sorusu olduğunda veya bir durumda ne yapacaklarını bilmediklerinde başvurduğu kişidir. Bu, onları nerede bulacaklarını, kime başvuracaklarını ve bir meslektaşı doğru desteğe nasıl yönlendireceklerini bildikleri anlamına gelir. KOBİ'lerde, özel BT personeli olmayan bu rol, çalışanların net bir referans noktası bırakmayacağı bir boşluğu doldurur.

- **Eğitimi ve sürekli öğrenmeyi teşvik etmek**. Change Agent, meslektaşlarını mevcut eğitim kaynaklarıyla etkileşime geçmeye teşvik eder; CyberAgent modülleri dahil, siber güvenlik alanındaki gelişmeler hakkında kurumun sektörü ve faaliyetleriyle ilgili gelişmelerden haberdar olur.
- **Geri bildirim toplamak ve yükseltmek**. Change Agent, çalışanların neleri kafa karıştırdığı, hangi uygulamaların takip edilmediği, hangi risklerin en acil göründüğü gibi organizasyon içindeki siber güvenlik endişeleri hakkında geri bildirim toplar ve bu içgörüleri yönetime sunar. Bu geri bildirim döngüsü, organizasyonun zaman içinde güvenlik kültürünü geliştirmesini sağlar.

Tablo 1. Teknik çalışanların görevleri ile Change Agent'in görevleri arasındaki ayrım

BT UZMANI (Teknik Rol)	SİBER GÜVENLİK YENİŞİK OYUNCUSU (Yönetici ve Kültürel Rol)
Güvenlik duvarlarını ve güvenlik sistemlerini yapılandırır	Özel farkındalık mesajları ve güvenlik uyarılarını meslektaşlarıyla paylaşır
Yazılım güncellemelerini, yamaları ve teknik yapılandırmaları yönetir	Siber güvenliği sürekli olarak takım içi toplantı gündemlerinde tutarlı tutar
Aktif siber olaylara ve teknik ihlallere yanıt verir	Meslektaşlarını şüpheli faaliyetleri aktif ve şeffaf şekilde bildirmeye teşvik eder
Ağ trafiğini, güvenlik kayıtlarını ve teknik uyumluluk parametrelerini izler	Yeni çalışanlara temel siber hijyen ile ilgili organizasyonel işe alım sürecinde destek verir

BT UZMANI (Teknik Rol)	SİBER GÜVENLİK YENİŞİK OYUNCUSU (Yönetici ve Kültürel Rol)
Teknik güvenlik kontrollerini uygular ve altyapı erişimini yönetir	Personelden sürekli geri bildirim toplar ve sistematik endişeleri yönetime veya BT'ye iletmektedir

3. SIBER GÜVENLIK DEĞIŞIM AJANI SEÇILIP ATANMAK

Siber Güvenlik Değişim Ajanı rolü için doğru kişiyi belirlemek ve ona başarılı olmaları için koşulları sağlamak, rolü bir organizasyon içinde uygularken alınması gereken kritik kararlardır. CyberAgent pilotu, bu rolün en iyi şekilde güvenilir biri tarafından doldurulduğunda işlediğini gösterdi; çünkü bu kişi güvenilir olarak algılanıyor, şirketin prosedürleri hakkında bilgi sahibi ve yönetim tarafından destekleniyor. Bu bölüm, uzun vadeli başarı için rolü net bir şekilde tanımlamak ve doğru adayı nasıl bulmak gerektiği konusunda pratik rehberlik sağlar.

3.1. DOĞRU ADAYI NASIL SEÇERIM

CyberAgent pilotunun sonuçlarına göre, en etkili Siber Güvenlik Değişim Ajanları mutlaka daha önce teknik geçmişe sahip olanlar değildir. Sekiz pilot ülke boyunca, eğitime en aktif katılan ve en büyük potansiyeli gösteren KOBİ katılımcıları, organizasyon farkındalığını iletişim becerileri ve gerçek motivasyonla birleştirerek iş yerlerinde fark yaratanlardı. Pilot deneyimine dayanarak, aşağıdaki özellikler roldeki başarıyı destekleme eğilimindedir:

- Kuruluşun iç süreçlerine ve veri işleme uygulamalarına aşinalık.
- İyi iletişim ve kişilerarası beceriler.
- Yönetimden destek

Önemli olarak, bu rol teknik veya BT geçmişi gerektirmez. Bu nedenle, idari rollerde, İK'da, operasyonlarda ve yönetimde çalışanlar, yeterli eğitim ve destek aldıkları sürece Değişim Ajanı işlevini etkili bir şekilde yerine getirebilirler. Teknik öncülün kaldırılması, uygun aday havuzunu önemli ölçüde genişleten ve pilot programın gösterdiği gibi cinsiyet çeşitliliğine kapı açan kasıtlı bir tasarım seçimidir.

Bir aday belirlendikten sonra, rol organizasyon içinde görünür ve meşru hale getirilmelidir. Rolün kapsamı organizasyon genelinde açıklanmalı ve net bir şekilde tanımlanmalıdır: Siber Güvenlik Değişim Ajanının sorumluluğu, kime rapor verdiği ve neler yapması beklenmediği açıkça belirtilmeli.

3.2. ROLÜN UYGULANMASI

Bir sonraki adım, bu rolü bir organizasyon içinde uygulamaktır. Aşağıdaki adımlar, CyberAgent pilotundan alınan derslerden doğrudan partner ülkeler genelinde yararlanmakta olup, her büyüklükteki KOBİ'ler için orantılı olacak şekilde tasarlanmıştır.

3.2.1. SIBER GÜVENLIK DEĞIŞIM AJANINI SEÇIN VE EĞITIN

Kuruluşunuzdaki en uygun kişiyi belirleyin ve ona CyberAgent eğitim programına erişim sağlayın. Program, Güvenlik Programı Yönetimi (M1), Sistem Yönetimi (M2), Analitik Araçlar (M3), Güvenlik Operasyonları (M4), Güvenlik Yönetişimi ve Politikası (M5), Siber Güvenlik Planlaması (M6), Risk Yönetimi (M7), İş Sürekliliği (M8) ve Siber Güvenlikte Kariyerleri Güçlendirme (M9) gibi dokuz modülden oluşmaktadır. Bu dokuz modül, resmi olarak iki resmi proje sunumunda yer almaktadır: D3.1, HEI müfredatını kapsıyor ve D3.2, VET müfredatını kapsıyor. Bu Rehberde referans verilen modüller, doğrudan D3.1 ve D3.2'de tanımlanan içeriğe karşılık gelir ve öğrenenin kurumsal bağlantısı ne olursa olsun CyberAgent platformu üzerinden erişilebilir. Ayrıca, müfredat KOBİ çalışanları için EQF 4-6 seviyelerine uygun olup, teknik, analitik, risk yönetimi ve organizasyonel yetkinlik alanlarında pratik uygulamalı temel siber güvenlik becerileri ve bilgileri sunmaktadır.

Eğitim kendi kendine ayarlanır ve çevrimiçi olarak sunulur; bu da seçilen çalışanın mevcut iş sorumlulukları çerçevesinde esnek bir şekilde tamamlaması anlamına gelir. Bir modülü tamamlayıp bilgi değerlendirme testini en az %75 puanla geçtikten sonra, Change Agent o modül için bir Kurs Tamamlama Sertifikası alır; bu sertifika, edinilen yetkinliklerin resmi bir kaydını sağlar ve Değişim Ajanının organizasyon içindeki eğitimini belgelemek için kullanılabilir.

3.2.2. SORUMLULUKLARI TANIMLAYIN VE MEVCUT YAPILARA ENTEGRE OLUN

Eğitim başladıktan veya tamamlandıktan sonra, organizasyon Siber Güvenlik Değişim Ajanının sorumluluklarını resmen tanımlamalı ve rolü mevcut yapılara entegre etmelidir. Bu, Değişim Ajanı'nın ne yapacağı, role ne kadar zaman ayıracağı ve kiminle koordinasyon yapacağı konusunda anlaşmak ve bunu tüm ekibe iletmek anlamına gelir.

Pilot program, Siber Güvenlik Değişim Ajanı rolünün en sürdürülebilir olduğu, organizasyonda zaten var olan bir şeyle bağlantılı olduğunda olduğu ve izole oturmak yerine olduğu gösterildi. Bu, bunu düzenli bir ekip toplantısı gündem maddesine bağlamak veya mevcut bir sağlık, güvenlik veya uyum yapısına bağlamak anlamına gelebilir. Amaç, siber güvenlik farkındalığını günlük işin normal bir parçası ve ortak bir organizasyon sorumluluğu haline getirmek, ayrı bir faaliyet değil.

3.2.3. ROL ETRAFINDA IÇ FARKINDALIK OLUŞTURUN

Değişim Ajanı, meslektaşları kim olduklarını veya ne yaptıklarını bilmezse etkili çalışamaz. Seçilen çalışana işlev görebilmesi için gereken organizasyonel meşruiyeti sağlamak için, rolü ve sorumluluklarını net bir iç iletişim göndermek ve çalışanların soru sormasına olanak tanıyacak düzenli toplantılar düzenlemek gerekir.

İlk duyurunun ötesinde, Change Agent'in düzenli toplantılarla kurum içinde siber güvenliği görünebilir tutması teşvik edilmelidir. Bu, uzun eğitim oturumları veya resmi sunumlar anlamına gelmez. KOBİ bağlamında, bu, çalışanların günlük işlerinden tanıdığı durumlarla doğrudan bağlantılı kısa faaliyetler şeklinde yapılabilir.

3.2.4. DÜZENLI OLARAK GÖZDEN GEÇIRIN VE ZAMANLA SÜRDÜRÜN

Siber Güvenlik Değişim Ajanı rolünün kalıcı etki yaratmasını sağlamak için, organizasyonun devam edip gelişmesi için gerekli koşulları yaratması gerekir. Bu, yılda en az bir kez bir inceleme süreci oluşturmak ve neyin işe yaradığını, hangi boşlukların kaldığını ve Değişim Ajanının ek eğitim veya desteğe ihtiyacı olup olmadığını değerlendirmek anlamına gelir.

Pilot kanıtları, sürekli etkileşimin sadece ilk eğitimden fazlasını gerektirdiğini gösteriyor. KOBİ katılımcıları, ivmeyi sürdürmek için esnek son tarihler, hatırlatmalar ve ara sıra desteğe ihtiyaç duyuyor. Basit bir yıllık inceleme eklemek ve Değişim Ajanının kaynaklara sürekli erişimini sağlamak, rolün zaman içinde etkili kalması için asgari koşullardır.

4. CINSIYET DENGESI VE KAPSAYICILIK

Siber güvenlik, Avrupa ekonomisinde en erkek egemen alanlardan biri olmaya devam ediyor. Kadınlar, AB genelinde siber güvenlik iş gücünün yaklaşık %20'sini oluşturuyor ve siber güvenlik eğitimine katılım da aynı dengesizliği yansıtıyor. Mevcut beceri ve yetenek açığı nedeniyle, mevcut havuzun sadece küçük bir kısmından yararlanan bir alan, mevcut tehdit çevresinin gerektirdiği talep ölçeğini karşılamakta zorlanacaktır.

CyberAgent projesi, cinsiyet kapsayımının açıkça bir hedef olarak tasarlandığı, sonradan düşünülmüş bir şey değil. Kadınların genellikle eğitim katılımcılarının küçük bir azınlığını oluşturduğu bir alanda, pilot programa katılan kadın katılımcıların yüksek olması anlamlı bir sonuçtur ve hedefli iletişim stratejileri ile kapsayıcı çerçeveleme ürünüdür.

4.1. NEDEN KOBİ'LER IÇIN ÖNEMLI

Özellikle KOBİ'ler için, siber güvenliğin cinsiyet boyutu hem bir iş gücü meselesi hem de organizasyonel kültür meselesidir. Çoğu KOBİ'nin özel siber güvenlik personeli yoktur. Siber dayanıklılıkları, özellikle idari, İK, finans ve operasyon rollerinde çalışanların farkındalığına ve davranışlarına bağlıdır. Bu nedenle, kadınları siber güvenlik farkındalık eğitiminden dışlamak bir güvenlik açığıdır.

Aynı zamanda, Siber Güvenlik Değişim Ajanı rolü, KOBİ'ler içinde siber güvenlikteki cinsiyet dengesizliğini ele almak için somut bir fırsat sunmaktadır. Rol, teknik uzmanlıktan ziyade iletişim becerileri, organizasyonel farkındalık ve yönetişim düşüncesi ile tanımlandığı için, geniş bir profesyonel profil yelpazesine iyi uyum sağlar ve teknik olmayan rollerdeki kadınlara kariyer değişikliği veya teknik yeterlilik gerektirmeyen siber güvenlik sorumluluğuna tanınmış bir yol sunar.

4.2. KADINLARA VE AZ TEMSIL EDILEN GRUPLARA ULAŞMAK IÇIN PRATIK ADIMLAR

Aşağıdaki pratik adımlar CyberAgent pilot deneyiminden alınmakta olup, her büyüklükteki KOBİ'ler tarafından uygulanabilir şekilde tasarlanmıştır.

Belçika'daki pilot program, kadınların zaten güvendiği mesleki dernekler ve iş kadını ağları gibi ağlar aracılığıyla iletişim kanallarının kadın katılımını artırdığını gösterdi. Pratikte bu, bir KOBİ'nin Siber Güvenlik Değişim Ajanı rolü için adaylar belirlerken, sadece kamu duyurularına dayanmak yerine, kendi sektörü veya bölgesiyle ilgili kadın mesleki ağlarıyla aktif olarak etkileşimde bulunması gerektiği anlamına gelir.

Rolü teknik uzmanlık değil, organizasyonel etki açısından çerçeveleyin. Teknik olmayan rollerdeki kadınlar, teknik becerilerden ziyade getirdiği organizasyonel değer açısından sunulduğunda siber güvenlik eğitimine katılma ve Değişim Ajanı işlevini üstlenme olasılığı daha yüksektir. Bu rol, işletmeyi koruyan, meslektaşları destekleyen ve yönetişime katkıda bulunan bir rol olarak çerçevelenebilir. İç iletişim, iş tanımları ve işe alım materyallerinde kullanılan dil önemlidir.

5. EN İYI UYGULAMALAR

Siber Güvenlik Değişim Ajanı atanmak önemli bir ilk adımdır, ancak bu rol ancak aktif olarak destekleyen bir organizasyon kültürü içinde çalışırsa kalıcı etki yaratabilir. Aşağıdaki en iyi uygulamalar, KOBİ'lerin Change Agent'in başarılı olması için doğru koşulları yaratmasına ve siber güvenlik farkındalığının organizasyonun çalışma biçiminin normal bir parçası haline gelmesine yardımcı olmak için tasarlanmıştır.

- **Açık iletişimi teşvik** edin. Çalışanlar, hataları, şüpheli durumları veya güvenlik endişelerini suçlanma veya utanç görme korkusu olmadan bildirmekte rahat hissetmelidir. Birçok kuruluşta, siber güvenlik olayları tam da çalışanların emin olmadıkları veya sorumluluk hissettikleri bir şeyi bildirmekte tereddüt etmeleri nedeniyle büyür.

- **Bunu basit ve günlük rutinlere entegre tutun**. Siber güvenlik farkındalığının resmi eğitim oturumları veya uzun atölye çalışmaları şeklinde olması gerekmez. Mevcut rutinlere gömülü kısa, pratik hatırlatmalar, ara sıra yoğun eğitimden daha etkilidir. Amaç, siber güvenliği periyodik bir olay yerine arka plan alışkanlığı haline getirmek.

- **Her adımı** belgeleyin. Bir KOBİ'nin atabileceği en pratik adımlardan biri, temel siber güvenlik uygulamalarını yazmaktır: şifrelerin nasıl yönetildiği, hassas verilerin nasıl saklandığı ve paylaşıldığı, şüpheli bir e-posta geldiğinde ne yapılacağı, bir olay durumunda kiminle iletişime geçileceği. Bunların resmi politika belgeleri olması gerekmez. Tüm çalışanların erişebileceği tek sayfalık bir referans yeterlidir.

- **En üstten başla**. Çalışanlardan beklenen davranışların yöneticiler ve liderlik tarafından gözle görülür şekilde modellenmesi gerekir. Yönetim temel güvenlik uygulamalarını takip etmezse, bu uygulamaların isteğe bağlı olduğunu gösterir. Değişim Ajanının organizasyon içindeki güvenilirliği, kısmen çevresindeki kültürün teşvik etmeye çalıştıkları şeyi destekleyip desteklemediğine bağlıdır.

- **Farkındalığı sürekli** kılın. Siber güvenlik tehditleri sürekli gelişir ve tek bir eğitim oturumu hızla geçer. Farkındalık, tek seferlik bir etkinlik değil, sürekli bir süreç olarak ele alınmalıdır. Bu, düzenli temas noktaları, periyodik tazelemeler ve güncel kalan ve güncel bilgileri kuruma geri getiren bir Siber Güvenlik Değişim Ajanı anlamına gelir.

5.1. ULUSAL PILOTLARDAN NITELIKSEL KATKILAR

Nitel geri bildirimler, katılımcıların genel olarak eğitime olumlu yaklaştığını ve birçoğu büyük bir iyileştirmeye ihtiyaç olmadığını belirtti. Açık metin yanıtlarında (D5.3 - CyberAgent Yetenek Geliştirme Eğitim Programı Değerlendirmesi) en çok tekrarlanan temalar şunlardı: platform kullanılabilirliği, navigasyon veya değerlendirme akışı; teknik erişim veya güvenilirlik sorunları; erişilebilirlik, esneklik ve geniş bilgi konusunda olumlu değer; daha pratik vakalar, uygulamalı laboratuvarlar veya gerçek KOBİ örnekleri talepleri; içerik yoğunluğu, yapı veya öğrenme yolu farklılaştırılması. Özellikle, en çok bahsedilen üçüncü tema (erişilebilirlik, esneklik ve geniş bilgi konusunda olumlu değer), katılımcıların herhangi bir iyileştirmeye ihtiyaç olmadığını belirten ve programın güçlü yönlerini istemeden vurgulayan takdirini yansıtmaktadır. Bu anlamlı bir sinyal: eleştiriyi yakalamak için tasarlanmış açık metin alanında, niteliksel yanıtların neredeyse dörtte biri eğitimin erişilebilirliği ve kapsamından memnuniyet duyduğunu ifade etti.

5.2. KOBİ'LERDE EĞITIMIN UYGULANMASI VE YÖNETIMI IÇIN EYLEM NOKTALARI

CyberAgent platformunun sekiz Avrupa ülkesinde geniş çaplı pilotlaştırılması, küçük ve orta ölçekli işletmelerin siber güvenlik becerilerini nasıl benimsediği ve sürdürdükleri konusunda önemli bilgiler sağladı. Nihai eğitim değerlendirme raporunda (D5.3) belgelenen karma yöntemli kanıtlar ve öğrenici engelleri temelinde, kurumsal yöneticilerin eğitimin organizasyonel etkisini optimize etmek için aşağıdaki iç yönetim, teknik ve stratejik eylem noktalarını benimsemeleri önerilir.

Kalite Yönetimi Tavsiyesi

CyberAgent öğrenme materyalleri, operasyonel ve stratejik bilgilerin önemli bir hacmi sunar. Yöneticiler, tüm müfredatı bir anda atamaktan kaçınmalıdır; Bunun yerine, modüler bir program oluşturmak, bilişsel yorgunluğu önler ve şirketin günlük rutinlerine daha sorunsuz bir yetenek geçişini sağlar.

Teknik Entegrasyon Tavsiyesi

İlk pilot veriler, gecikmeli veya filtrelenmiş platform kayıt onay e-postaları gibi teknik işe alım sorunlarının erken benimsenmeyi engelleyebileceğini kaydediyor. Kullanıcı kaydını başlatmadan önce, yönetim harici e-öğrenme alan yollarının tamamen izin verildiğinden emin olmak için ağ filtreleriyle koordinasyon sağlamalı ve personele temel spam klasörlerini izlemelerini tavsiye etmelidir.

Stratejik Konuşlandırma Tavsiyesi

Ulusal pilot veriler, özellikle M6 (Siber Güvenlik Planlaması) ve M8 (İş Sürekliliği) gibi daha üst düzey stratejik modüllerin tam anlamıyla kullanılabilmek için sağlam bir altyapı deneyimi gerektirdiğini ortaya koydu. Anında iş değerini en üst düzeye çıkarmak için, bu modüller özellikle yönetimsel, operasyonel veya iş yönetimi sorumluluklarına sahip personele yönelik olmalıdır.

5.2.1. DEĞIŞIM AJANININ SESI

Sekiz Avrupa ülkesinde 272 kapsamlı anket yanıtını toplayan pilot aşama, hedef gruplar üzerinde üç çapraz etki ortaya koydu.

Yüksek Teslimat Esnekliği ve İş-Çalışma Dengesi

Katılımcıların önemli bir %86,0'ı, asenkron, kendi hızında ilerleyen formatın profesyonel ve akademik programlarına sorunsuz entegre edilebilecek kadar esnek olduğu konusunda hemfikir veya kesinlikle hemfikir oldu; bu da KOBİ çalışanlarının yeterlilik geliştirme ile günlük operasyonel görevleri arasında denge kurmasına olanak tanıdı.

Teknik Olmayan Personel için Metodolojik Önem

Pilot sonuçlar, CyberAgent müfredatının temel eğitim tasarımını doğrular ve etkili organizasyonel siber dayanıklılığın ileri teknik veya BT programlama becerileri gerektirmediğini kanıtlar. D5.3'teki etki değerlendirme verilerine göre, katılımcıların %77,2'si eğitimin, belirli mesleki rollerinin bir işletme içindeki günlük güvenlik uygulamalarını nasıl etkilediğini ve korunduğunu net bir şekilde anlamalarını sağladığını bildirdi.

Uzman Olmayan Temellerden Ölçülebilir Bilgi Gelişimi

Platform analizleri, katılımcıların %89,3'ünün siber güvenlik bilgisinde doğrulanmış bir artış sağladığını gösteriyor. Önemli olarak, bu ilerleme en çok yeni başlayanlar arasında belirgindi: programdan önce ilk anlayışlarını "Çok Düşük" olarak değerlendiren öğrencilerin %90,9'u, kurumsal siber riskleri tanıma bilgisi ve özgüvenlerinde belirgin bir artış olduğunu bildirdi.

5.2.2. "YAPILMASI VE YAPILMAMASI"

Pilot ülkelerden gelen "öğrenme yolu farklılaştırması" konusundaki geri bildirimlere dayanarak, şirketler için öneriler sunuyoruz:

Tablo 2 "Yapılmalı ve Yapılmalı"

YAPMA (SME Tuzakları)	TAVSIYE EDİLEN (En İyi Uygulama)
Bir çalışanın tüm 8 modülü gerçekçi olmayan, sıkıştırılmış bir zaman diliminde (örneğin bir hafta veya ay) dinleyeceğini beklemek. Pilot çalışmalar (D5.3), günlük iş sorumlulukları nedeniyle zaman eksikliğinin KOBİ çalışanları için ana engel olduğunu ve sınav geçme oranının daha düşük olmasına yol açtığını ortaya koydu.	Çalışanın ihtiyaçları ve erişilebilirliğine göre esnek, bireysel bir öğrenme programı oluşturmak, mikro-öğrenme ilkelerini uygulamak. Öğrencilerin, işyeri etki alanlarını doğrudan artıran modüllere odaklanmalarına izin verin.
Eğitilmiş Siber Güvenlik Değişim Ajanının uzmanlaşmış BT mühendisliğini değiştireceğini veya karmaşık siber olayları bağımsız olarak çözeceğini beklemek. Temel teknik altyapı beklentilerinin teknik olmayan personele kaydırılması büyük rol belirsizliği yaratır.	Değişim Ajanını iç güvenlik koordinatörü ve farkındalık katalizörü olarak hareket etmeye teşvik etmek. En etkili olarak, güvenlik kültürünü, iç eğitim hatırlatıcılarını kullanırken ve takım toplantılarında kısa güncellemeler yaparken.
E-öğrenme sürecini tamamen izlenmeden bırakıp kurumsal görünürlük olmadan otomatik pilotta çalışmaya zorlamak. Tek bir kayıt bağlantısı, uzun vadeli organizasyon değerini garanti etmez.	Dönüm noktalarını takip etmek ve dahili mentorluk atamak için yapılandırılmış izleme çerçevesini (örneğin Tablo 3) kullanmak. Pilot değerlendirmesinden (D5.3) alınan ipuçları, belirlenmiş bir yönetici veya mentorun olmasının doğrulanmış test kesinleştirme ile açıkça ilişkili olduğunu doğrular.
Bağımsız çalışmanın tamamen izole olmasına izin vererek, bireysel öğrenme engellerinin veya gizli teknik zorlukların fark edilmemesi riskini artırır. Etkileşim olmadan, mutlak yeni başlayanlar genellikle takıldıklarında programı sessizce bırakıp oyalıyorlar.	Kendi hızında çalışmaları, kısa nabız kontrolleri veya dijital hatırlatmalar gibi proaktif operasyonel temas noktalarıyla entegre etmek. Aktif yönetim uyumu, öğrenme engellerini doğrudan ortadan kaldırır, çalışan motivasyonunu ve ders tamamlama oranlarını yükseltir.

6. SIBER GÜVENLIK DEĞIŞIM AJANINI UYGULAMAK IÇIN YOL HARİTESI

Siber Güvenlik Değişim Ajanı rolünün başarılı bir şekilde uygulanması, atamadan çok önce başlar. Kuruluşun mevcut durumunu değerlendirmek, iç destek oluşturmak ve rolü baştan net bir şekilde tanımlamak için zaman ayırmak, uzun vadeli başarı şansını önemli ölçüde artırır. Aşağıdaki adımlar, KOBİ'leri bu hazırlık aşamasında pratik olarak yönlendirmek için tasarlanmıştır.

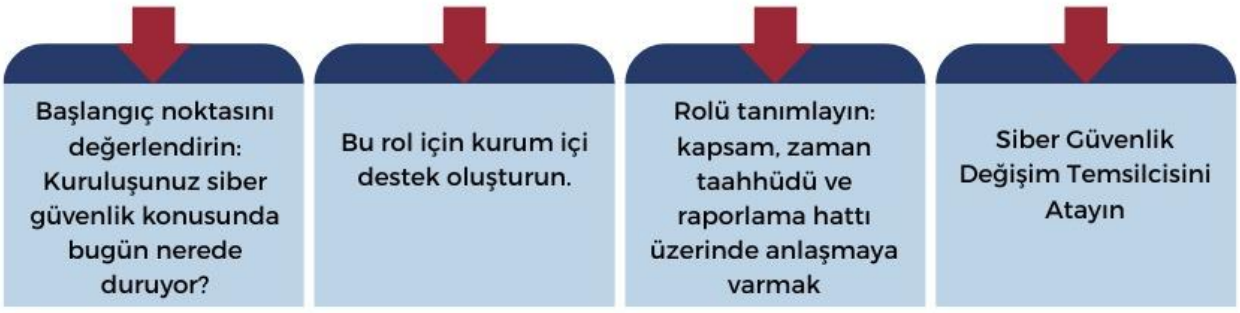
1. İlk adım, kuruluşun şu anda nerede durduğunu değerlendirmek. Bu, zaten var olan veya olmayan siber güvenlik uygulamalarına dürüstçe bakmak anlamına gelir. Çalışanlar, oltalama gibi temel tehditlerin farkında mı? Şüpheli olayların bildirilmesi için bir prosedür var mı? Hassas veriler ekip genelinde tutarlı şekilde ele alınıyor mu?

2. İkinci adım, rol için iç destek oluşturmaktır. Değişim Ajanı, yönetim desteği olmadan etkili çalışamaz. Bir aday seçilmeden önce, rolün tanıtılması kararı yönetim düzeyinde tartışılı ve kabul edilmeli; zaman ayırma, rolü resmi olarak tanıma ve görevi üstlenen kişiyi aktif olarak destekleme konusunda net bir taahhüt gösterilmelidir.

3. Üçüncü adım, rolü doldurmadan önce tanımlamak. Bu, sorumlulukların kapsamı, beklenen zaman taahhüdü ve rolun mevcut organizasyon yapısı içinde nasıl yer alacağı konusunda anlaşmak anlamına gelir. Açık bir yetki, basit bir paragraflık açıklama bile olsa, belirsizlikten kaçınır ve gelecekteki Siber Güvenlik Değişim Ajanına harekete geçmesi için gereken meşruiyeti sağlar.

Ancak bu üç adım uygulandığında, organizasyon doğru adayı belirlemeye ve atamaya hazır olur. Aşağıdaki bölüm, rolün başarılı bir şekilde uygulanmasına rehberlik edecek kontrol listesini özetlemektedir.

Şekil 1 - Siber güvenlik değişim ajanını uygulamak için Görsel Yol Haritası



7. KONTROL LISTESI

Aşağıdaki kontrol listesi, başarılı bir Siber Güvenlik Değişim Ajanı uygulaması için temel koşulların sağlanıp sağlanmadığını doğrulamak amacıyla tasarlanmıştır. CyberAgent pilotundan alınan derslere dayanıyor.

7.1. YÖNETIM

[ ] Değişim Ajanı rolü resmi olarak anlaşıldı ve bütçelendi.

[ ] Net bir yetki tanımlandı: kapsam, zaman taahhüdü ve raporlama hattı

[ ] Atama tüm kuruluşa iletildi

[ ] Rolün gözden geçirilmesi önümüzdeki 12 ay içinde planlandı

[ ] Değişim Ajanı, rolü yerine getirmek için programında korunan zaman ayırmıştır

7.2. İNSAN KAYNAKLARI

[ ] Seçim süreci, cinsiyet veya geçmiş fark etmeksizin herkese açıktı

[ ] Rol, teknik uzmanlık değil, organizasyonel etki açısından iletildi

[ ] Değişim Ajanının sorumlulukları, iş tanımında veya amaçlarında yansıtılmıştır

[ ] Yeni çalışanlar, işe başlama sırasında Siber Güvenlik Değişim Ajanı ile tanıştırılır

[ ] Değişim Ajanının eğitimi ve sertifikalarının kaydı tutulur

7.3. SIBER GÜVENLIK DEĞIŞIM AJANI

[ ] CyberAgent platformuna kayıt oldu ve bir öğrenme yolu üzerinde anlaştık

[ ] En az bir modülü tamamlayıp bir sertifika aldı

[ ] Meslektaşlar Değişim Ajanı ile nasıl iletişime geçileceğini bilir

[ ] Temel siber güvenlik uygulamaları belgelenmiş ve tüm personel için erişilebilir

[ ] Düzenli farkındalık temas noktaları (toplantılar, mesajlar veya hatırlatmalar) yerindedir.

[ ] Şüpheli durumları bildirmek için meslektaşların net bir süreci vardır

[ ] Siber güvenlik endişeleriyle ilgili geri bildirimler düzenli olarak toplanır ve yönetime iletilir

8. BAŞARILI BIR UYGULAMAYI NASIL ÖLÇERIM

Siber Güvenlik Değişim Ajanı rolünün uygulanması sürekli bir taahhüttür. Aşağıdaki göstergeler, KOBİ'lerin rolün zaman içinde gerçek bir etkisi olup olmadığını değerlendirmelerine yardımcı olabilir.

[ ] Değişim Ajanı atandığından beri siber güvenlik farkındalık faaliyetlerine katılan çalışanların sayısı arttı

[ ] Siber güvenlik, ekip toplantılarında düzenli olarak gündeme getiriliyor ve artık istisnai bir konu olarak ele alınmıyor

[ ] Çalışanlar Değişim Temsilcisinin kim olduğunu bilir ve soruları veya endişeleri için onlara rahatça yaklaşırlar

[ ] Bildirilen şüpheli e-postalar, olaylar veya endişeler sayısı arttı

[ ] Değişim Ajanı, ilk atamalarından bu yana ek eğitim modüllerini tamamlamıştır

[ ] Kuruluş içindeki siber güvenlik personel geri bildirimleri periyodik olarak toplanır ve uygulanır

8.1. ŞABLON UYARLAMASI VE ÖZELLEŞTIRME İÇIN YÖNETICI REHBERLIĞI

Siber Güvenlik Değişim Ajanının becerilerini geliştirmesinin uzun vadeli kurumsal dayanıklılığa aktarılmasını sağlamak için sürekli yapısal izleme gereklidir. Tablo 3, KOBİ yöneticilerinin eğitimden önce organizasyon temel seviyelerini değerlendirmeleri ve atamadan 6 ile 12 ay sonra somut güvenlik kültürü ilerlemesini ölçmeleri için tasarlanmış pratik bir takip şablonu sunar.

Yöneticiler bu şablonu dinamik bir çerçeve olarak ele almalıdır. Şirketinizin büyüklüğüne, operasyonel sektörüne ve mevcut altyapısına bağlı olarak, bu matrisi uyarlamanız ve genişletmeniz teşvik edilir:

- **Ölçekleri Özelleştirmek**
  Mikro-KOBİ'ler (10 çalışmadan küçük), takibin kolaylığını korumak için yüzdeye dayalı metrikleri doğrudan çalışan sayımlarına dönüştürebilir.
- **Genişleyen Göstergeler**
  Yüksek dijitalleştirilmiş veya yüksek riskli ortamlarda çalışan işletmelere, "Çok faktörlü kimlik doğrulama (MFA) kullanan personelin %'si" veya "Simüle edilmiş bir tehdide ortalama yanıt süresi" gibi hedefe özgü satırlar eklemeleri önerilir.
- **Yerelleştirme**
  "Önerilen Veri Kaynağı" sütununu kendi iç iletişim kanallarınızla hizalayın (örneğin, Slack üzerinden izleme, MS Teams anketleri veya ekip brifingleri sırasında fiziksel kayıtlar).

Tablo 3. KOBİ Yöneticileri için Randevu Sonrası Takip Şablonu

Başarı Göstergesi	Birim / Ölçü Ölçeği	Temel (Önce)	İlerleme (6 Ay)	Hedef (12 Ay)	Önerilen Veri Kaynağı
Çalışan Oltalama Hazırlığı	Şüpheli e-postaları ele almakta çalışanların %'i	%	%	%	İç nabız anketi veya CyberAgent platform verileri
Toplantı Entegrasyon Sıklığı	Siber güvenliğin gündeme getirildiği ekip toplantılarının sayısı	Kont	Kont	Kont	Takım toplantı tutanakları/gündemleri
Olay Bildirimi Aktif Oranı	Bildirilen Şüpheli Olayların Sayısı	Sayım / ay	Sayım / ay	Sayım / ay	İç güvenlik olay günlüğü veya BT geri bildirim döngüsü
Change Agent Görünürlüğü	Değişim Ajanının kim olduğunu doğru şekilde bilen personelin %'i	%	%	%	Kısa iç anket
Platform İlerleme Taahhüdü	Mikro-öğrenmeye aktif olarak katılan çalışan sayısı	Kont	Kont	Kont	CyberAgent platform yöneticisi analitik kontrol paneli

SONUÇ

Siber güvenlik, özel BT departmanları olan büyük kuruluşlara özgü bir endişe değil. Tehdit ortamı gelişmeye devam ettikçe ve KOBİ'lere yönelik düzenleyici beklentiler artarken, asıl soru onların sahip oldukları kaynaklarla kendilerini nasıl savunabilecekleridir.

Siber Güvenlik Değişim Ajanı rolü, bu soruya pratik ve orantılı bir cevap sunuyor. Bir uzman tutmak, pahalı aletlere yatırım yapmak veya mevcut süreçleri yeniden düzenlemek gerektirmez. Bu, kuruluş içinde doğru kişiyi belirlemeyi, onlara eğitim ve hareket yetkisi verilmesini ve siber güvenlik farkındalığının günlük çalışma yaşamının bir parçası haline gelmesi için koşullar yaratmayı gerektirir.

CyberAgent projesi bunun mümkün olduğunu gösterdi. Sekiz Avrupa ülkesinde, teknik geçmişi olmayan KOBİ çalışanları eğitimi tamamladı, görevi üstlendi ve kuruluşlarının siber güvenliğe yaklaşımında fark yaratmaya başladı. Kanıtlar açıktır: giriş engeli indirildiğinde, rol teknik uzmanlık yerine organizasyon kültürü etrafında şekillendiğinde ve kapsayıcılık bir tasarım ilkesi olarak ele alındığında, sonuçlar ortaya çıkar.

Bu Rehber, o ilk adımı atmaya bir davet. Yol haritası orada. Araçlar mevcut. Bu rol, çalışanlarına yatırım yapmak isteyen her KOBİ için ulaşılabilir.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Ajan-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM Grupo

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

IT Akademija

ProxyLab

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau