KASPERSKY lab

SİBER GÜVENLİK FARKINDALIĞI

www.kaspersky.com.tr

Siber Güvenlik Farkındalığı

KİM FAYDALANABİLİR

Bu kurslar özellikle aşağıda belirtilen kişilere faydalı olacaktır:

- İşletme Yöneticileri,
- Bölgesel BT Güvenlik görevlileri,
- Önemli veriler ve dış bağlantılar ile çevrim içi çalışan herkes.

Online etkileşimli eğitim modülleri ve site üzerinden CyberSafety Games eğitim programları, iş yerinde, bilgisayar veya mobil cihaz kullanan ve bunları yöneten tüm çalışanlar için dizayn edilmiştir.

ÖĞRENİME YAKLAŞIM

Siber vakaların %80'i insan hatasıyla meydana gelmektedir. Şirketler siber güvenlik farkındalığı için milyonlar harcıyor ancak çok az sayıda CISO (Bilgi Güvenliği Yöneticisi) sonuçlardan tatmin olmakta. Sorun ne? Çoğu siber güvenlik farkındalığı eğitimleri çok uzun, teknik içerikli ve sıkıcıdır. Bu tarz eğitimler, insanların temel yönlerine ulaşamıyor – karar verme prensipleri ve öğrenme becerilerine – ve sonuç olarak eğitimi faydasız hale getiriyor.

Dolayısıyla işletmeler, güvenlik farkındalığına yaptıkları yatırım için, ölçülebilir ve daha derin içerikli harcamalara değecek geri dönüşler sağlayacak davranışsal yaklaşımları (kurumsal kültür gelişimi gibi) arıyor. Kaspersky Lab CyberSecurity Awareness eğitimleri şu şekilde çalışır:

- Davranış değiştirme - bireyin güvenli çalışmaya bağlılığını uyarıcı, "Herkes siber güvenliğe dikkat ediyor, o halde ben de etmeliyim" düşüncesiyle gelişen bir kurumsal yapının kurulması.
- Motivasyona yönelik bir yaklaşım, oyunla öğrenme teknikleri, tasarlanmış saldırılar ve derinlemesine etkileşimli siber güvenlik becerileri eğitimini birleştirmek.

Kapsamlı, basit ve anlaşılır	Eğitim, İnternet kaynaklı zararlı yazılım saldırıları yüzünden nasıl veri sızdığından güvenli sosyal ağlara, geniş bir güvenlik sorunları yelpazesini, BT-dışı insanlara uygun bir dille bir dizi basit egzersiz aracılığıyla işler. Grup dinamikleri, interaktif modüller, karikatür ve oyunlaştırma gibi eğitim teknikleri kullanarak, eğitimi çekici hale getiriyoruz.
Sürekli Motivasyon	Oyunlaştırma ve yarışmalarla öğretilebilir anlar yaratıyoruz ve bu anları, tasarlanmış ataklarla, değerlendirmelerle ve eğitim görevleriyle yıl içinde pekiştiriyoruz.
Bakış açısının değişmesi	Siber suçluların asıl hedefinin bilgisayarlar değil, insanlar olduğunu öğretiyoruz. Bireyin, güvenlik bilinci anlayışıyla çalışarak, kendini ve iş yerini ifşa etmekten ve mağdur olmaktan nasıl korunacağını gösteriyoruz.
Kurumsal bir siber güvenlik kültürü oluşturmak	Yönetimi eğitip, birer güvenlik savunucusu haline getiriyoruz. Siber güvenliğin günlük hayatın bir parçası haline geldiği bir kültüre erişmenin en iyi yöntemi, yönetimin kararlılığı ve örnek olmasıdır, sadece IT tarafından dayatılması bir işe yaramaz.
Olumlu ve İşbirlikçi	Güvenlik uygulamalarının, iş verimliliğine nasıl olumlu katkıda bulunduğunu. IT Güvenliği ekibi de dahil olmak üzere tüm departmanlarla daha etkin ve ortak bir çalışmanın nasıl teşvik ettiğini gösteriyoruz.
Ölçülebilir	Çalışan becerilerini ölçmenin yanı sıra, çalışanların günlük işlerinde siber güvenliğe karşı tutumlarını inceleyen kurumsal seviyede değerlendirmeler sunan araçlar sağlıyoruz.

PROGRAMIN FAYDALARI

Kaspersky CyberSecurity Awareness eğitimi zihinleri değiştirir, gerçek hayattaki olaylar aracılığıyla güvenlik odaklı davranışları teşvik eder ve iş yerinde siber güvenlik ile ilgili en iyi uygulamaları kullandırır.

Yakın zamandaki bir çalışmanın sonuçlarına göre:

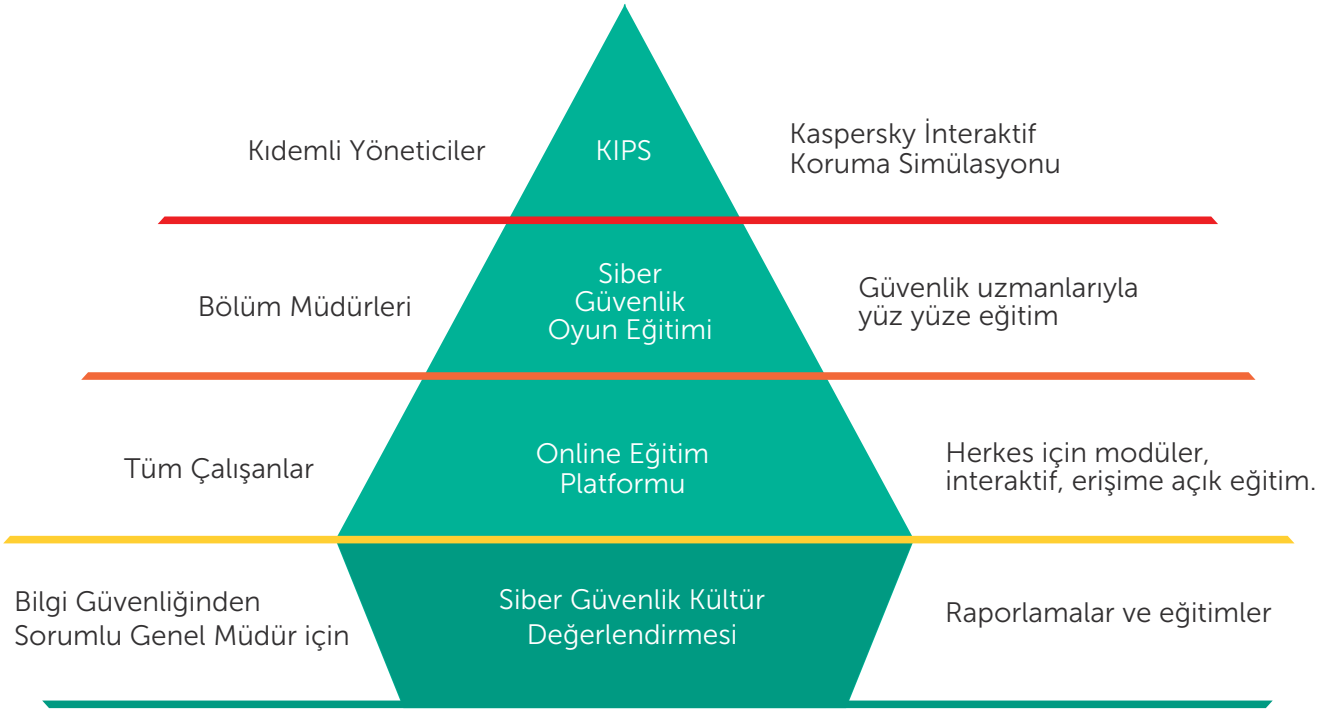
- Güvenlik farkındalık programı olan şirketler, bu eğitimi almamış rakiplerine nazaran, güvenlik vakalarına % 76 daha az para ödüyor. (Yıllık ortalama mali kayıp $162,000'a karşı $683,000).
- Güvenlik farkındalık programını almış şirketlerde, çalışan kaynaklı güvenlik ihlalleri %50 daha az görülüyor.

  Etkin bir CyberSecurity Awareness Programı'nın değeri:

  - Vaka sayısını %90 oranında düşürür.
  - Siber risk maliyetini %50-60 azaltır.
  - Sibergüvenliği bilişim jargonundan iş diline tercüme eder ve iş yönetiminin 'işe girmesini' sağlar.
  - Güvenlik farkındalığıyla ilgili ölçülebilir sonuçlar çıkarır.

KURS İÇERİĞİ

Kaspersky Lab CyberSecurity Awareness eğitimi birbirine bağlı bileşenden oluşur. Bu bileşenler ayrı ayrı kullanıldıklarında da tamamen etkindir.



Kaspersky Siber Güvenlik Farkındalık Eğitiminin Yapısı

[1] ABERDEEN GROUP. The Last Mile in IT Security: Changing User Behaviors, ABERDEEN GROUP, October 2014

ONLINE YETENEK GELİŞTİRME PLATFORMU

Bilgiler ve becerilerin üzerine yenilerini eklemek önemlidir, bu yüzden çevrimiçi bir veriler platformuna katılımcıların tipik senaryo ve durumlar üzerinde çalışıp daha fazla bilgi kazanmasını sağlamak, olası tehditleri anlayarak bunlarla nasıl başa çıkılacağını öğrenmek için esastır. Kaspersky CyberSecurity Awareness Training eğitiminin ana öğeleri şunlardır:

- **Yetenek Değerlendirmesi:** Kullanıcının kendi yeteneklerini ve eğitim gereksinimlerini belirlemek içindir. Birçok güvenlik alanını kapsamaktadır. İçerisinde önceden tanımlanmış veya rastgele değerlendirme sınavları, müşteri tarafından belirlenmiş sorular ve gereksinime göre ayarlanabilir sürelendirme bulunmaktadır.
- **Eğitim Modülleri:** Kimlik avından korunma, Veri Koruma ve Yok Etme, Güvenli Sosyal Ağlar, Fiziki Güvenlik, Akıllı Telefon Güvenliği, Daha Güvenli Web Tarayıcısı, Ofis dışında da Güvenlik, Sosyal Mühendislik, URL Eğitimi, e-Posta Güvenliği, Şifreler.
- **Tasarlanmış Saldırılar:** Farklı zorluklarda, göndermeye hazır, uyarlanabilir, çok çeşitli kimlik avı saldırısı e-postaları. Yapılan kimlik avı saldırısına yenik düşen firma çalışanı, uzantının üzerine tıkladığı zaman otomatik olarak ilgili eğitim modülüne kaydı yapılır.
- **Analiz & Raporlama:** Göreve, Gruba, Cihaz türüne, Tekrarlayan Saldırgana, Konuma göre sonuçlar. Ek olarak, destekleyici güvenlik posterleri, e-posta şablonları, ekran koruyucular.

Online Eğitim adayların etkileşimli eğitim platformu üzerinden pratik yapmasını ve öğrenmesini sağlar.

Bu portalı Kaspersky En İyi Uygulamalar Rehberi eşliğinde kullanarak, Eğitim Yöneticisi güçlü, sürekli ve ölçülebilir bir sibergüvenlik eğitim planı uygulayabilir, çalışanları en basit kavramlardan en karmaşıklarına taşıyabilir, eğitim öğelerini bireysel becerilere ve tehdit ortamlarına göre şekillendirebilir.

CYBERSAFETY GAMES EĞİTİMİ

Bu son derece etkileşimli çalışma, Kaspersky Lab'ın kalifiye eğitmenlerinden biri tarafından yönetilir ve adaylara gerçek siber tehditler üzerinden, senaryo tabanlı bir yaklaşımla temel bilgileri sunar.

Sunum, adayların günlük olayları, başka hiçbir sağlayıcının sunamayacağı şekilde son saldırılar ve kötü amaçlı yazılımlara dair etkileşimli, pratik bir deneyimle keşfeder. Program, güvenliği ve çalışanların günlük işe eylemleri sırasında siber tehditlere dair farkındalığını artırmayı stratejik bir gereksinim olarak gören şirketler için özel olarak geliştirilmiştir.

EĞİTİM, BÖLÜM MÜDÜRLERİNİ MOTİVE EDER:

- "Neden güvenliğe önem vermeleri gerektiğini" anlamaya;
- Güvenli ve güvensiz davranış arasındaki farkları ayırt etmeye (teknik ve tedbirsel yetenekler);
- Program sadece "Bunları Yapmayın" diyerek değil "Bunları Yapın" diyerek olumlu örneklerle öğretir;

Ve adayların, siber suçluların kendilerini nasıl gördüklerini anlamalarını sağlar. Değer: %93 - eğitimde edinilen bilgiyi günlük işlere uygulama olasılığı[1].

Sunan:

- Eğitim Kaspersky eğitmeni tarafından verilir
- Eğitmeni eğitmek (şirket içindeki eğitimleri verme lisansı ve eğitimi)

Mevcut formatlar:

- 2şer saatlik oturumlar dizisi
- Tam gün oturum

Bakış açısını değiştirmek

Biz insanlara siber suçluların asıl hedefinin makineler değil insanlar olduğunu öğretiyoruz. Bireyin, güvenlik bilinci anlayışıyla çalışarak, kendisini ve iş yerini saldırılara açık bırakmaktan ve mağdur olmaktan nasıl korunacağını gösteriyoruz.

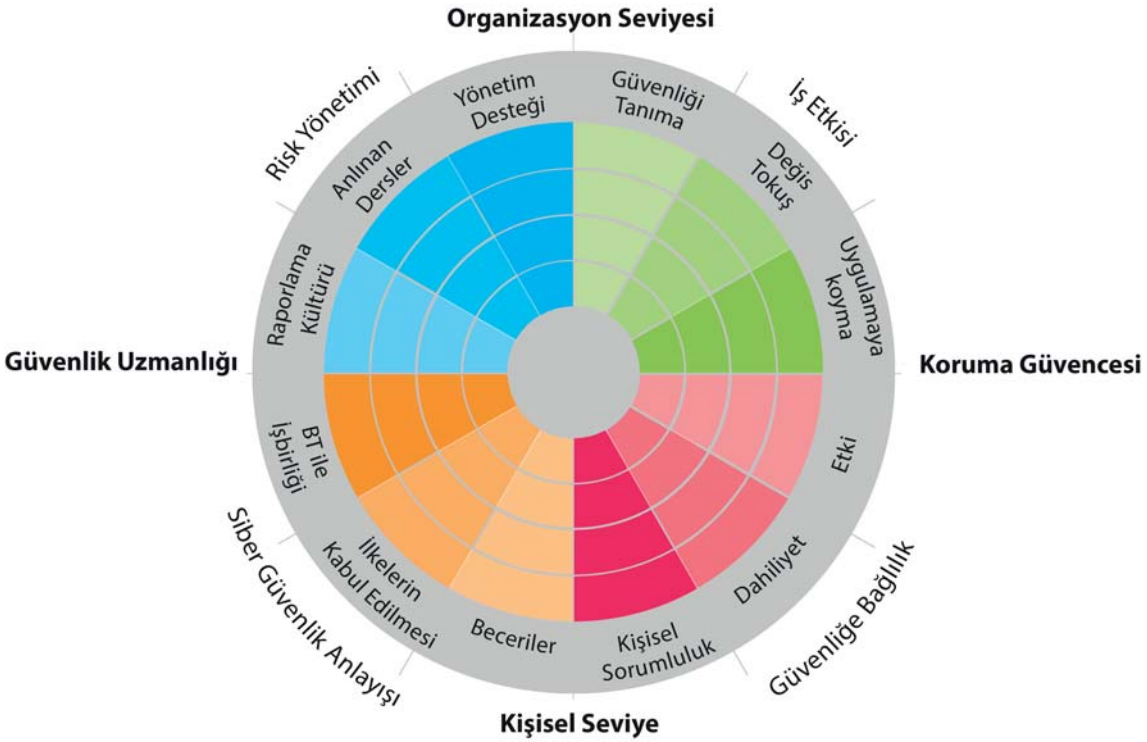
Yanlış inançları	Yeterli algılara ve	Olumlu rol modellerine dönüştürmek
Akıllı hacker virüsü gönderip bilgisayarımı bozacak	Bozuk bilgisayarlardan değil, kötü insanlardan korkun	Dijital varlıklarımdan hangi suçluların değer elde edebileceğini biliyorum, bu yüzden onları koruma motivasyonum var.
Çok küçük bir hedefim.	Küçük hedefler suçlular için daha kolay ve kimi zaman daha çekicidir	Diğerlerinden daha zor bir hedef olmak istiyorum.
Güvenlik için zamanım yok	Güvenlik uzun vadeli verimliliğin bir parçasıdır.	İş hedeflerine ulaşmanın en güvenli yöntemini seçeceğim ve güvenlik ekibiyle işbirliği yapacağım.

[1]SiberGüvenlik Oyunları eğitimlerini kullanan Kaspersky Lab müşterilerinin vaka değerlendirmelerinden elde edilen veriler.

SİBER GÜVENLİK KÜLTÜRÜ DEĞERLENDİRMESİ

Siber Güvenlik Kültürü Değerlendirmesi, şirketin her kademesinde siber güvenliğe yönelik günlük tutum ve davranışları analiz eder ve organizasyonunuzda çalışanların siber güvenliği nasıl farklı bakış açılarından algıladığını gösterir.

Ortaya çıkan rapor dengesizlikleri ve daha çok odaklanılan bölgeleri anlamak, Güvenlik Departmanının dahili ve harici etkinliklerinin (farkındalık ve eğitim, dahili halkla ilişkiler ve bilgi paylaşımı ve işler sürerken ortaya çıkacak diğer işbirliği ilkeleri gibi) önceliklerini belirlemeye ve gerekçelendirmeye yardımcı olmak amacıyla kullanılabilir.



AYDINLIK TARAFA GİDEN YOL EĞİTİMİ

Edinilen beceriler ve öğrenilen gereçler:

- Güvenlik farkındalığı mesajlarıyla kullanıcılar nasıl etkilenebilir;
- Direnç ve cehaletin üstesinden nasıl gelinir;
- %90 politika kabulü ve uyumuna nasıl erişilir.

Eğitim kullanıcıların kalplerine ve zihinlerinize giden yolları bulmanıza yardımcı olur. Daha güvenli davranışlara geçiş, bilinçli seçimlerden doğar.

Eğitim, grup çalışmaları sayesinde size tipik "güvensiz" durumları farklı açılardan görme imkanı sağlar. Bunun ardından mesajınızı doğru seçimleri ve kullanıcı tavırlarındaki doğru değişimleri sağlayacak şekilde yapılandırabilirsiniz.

Bu eğitim Kaspersky Güvenlik Farkındalığı portföyünün parçasıdır ve Siber Güvenlik Kültürü yöntemine dayanır.

Sunan:

- Kaspersky eğitmeni tarafından verilen 4 saatlik eğitim

KASPERSKY İNTERAKTİF GÜVENLİK SİMÜLASYONU (KIPS)

Güvenliğin önündeki en büyük engellerden biri, farklı üst yönetim görevlerinin siber güvenliği farklı açılardan görmesi ve farklı önceliklere sahip olmasıdır. Bu, şöyle bir karar alma ile sonuçlanabilir "Güvenlik Bermuda Şeytan Üçgeni"

- İşletmeciler, güvenliği iş hedefleri yolunda karmaşık/aykırı olduğunu düşünebilir (daha ucuz/daha hızlı/ daha fazla/daha iyi);
- BT güvenlik yöneticileri siber güvenliğin altyapı ve yatırım meselesi olduğunu ve kendilerini aştığını düşünebilir;
- Maliyet kontrolü görevini üstlenen yöneticiler, siber güvenliğe yapılan harcamaların gelirlerle nasıl bir ilişkisi olduğunu ve maliyet yaratmak yerine maliyetten nasıl koruduğunu anlamayabilirler.

Bu üçü arasındaki karşılıklı anlayış ve iş birliği, başarılı bir siber güvenlik için kritik önemdedir. Ancak, dersler ve kırmızı/mavi egzersizleri gibi geleneksel farkındalık formatları sorunludur: - uzun, aşırı teknik ve meşgul yöneticilere uygun değildir. "Sağduyu" seviyesinde "ortak dil" üretmeyi başaramazlar.

ÇÖZÜM: KIPS

KIPS'in amacı farklı karar verme alanlarından bu üst düzey profesyonelleri bir araya getirip, işletmenin bir bütün olarak çıkarları doğrultusunda çalışmaları esnasında birbirlerinin sorumluluklarını, amaçlarını ve endişelerini anlamalarını sağlamaktır.

BT, İşletme ve Güvenlik için - siber güvenlik karar mercileri için strateji simülasyonu.

- Eğlenceli, cazip ve hızlı (2 saat)
- Takım çalışması bölümler arası işbirliğini geliştirir.
- Rekabet, girişimcilik ve analiz yapma yeteneklerini geliştirir.
- Oyun oynamak bir siber güvenlik ölçümleme ve strateji anlayışı oluşturur.

Takımlar kurgulanmış bir girişimi yürütüp para kazanarak yarışırlar.

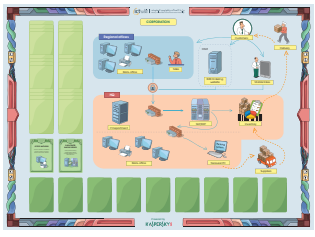
Firma siber saldırıyı deneyimlerken oyuncular atağın üretim ve gelir üzerindeki etkisini deneyimler. Farklı bakış açılarından, BT stratejileri ve çözümleri ile atağın zararını en aza indirmeye çalışır ve daha fazla para kazanmayı öğrenir. Mevcut senaryoların kapsamı:

Endüstriel: Su Tedarik

Finansal

Hükümet

Kurumsal



KIPS oyununu oynadıktan sonra oyuncuların günlük iş faaliyetleriyle ilgili, harekete geçirilebilir, önemli çıkarımlara varmış olurlar.

- Siber saldırılar gelirlere zarar verir ve üst yönetim seviyesinden ilgilenilmeleri gerekir.
- BT Güvenliği ve Şirket Departmanları arasında işbirliği, başarılı siber güvenlik için esastır.
- Güvenlik maliyetleri milyonları bulmak zorunda değildir, ve kaybetme riskine girdiğiniz gelire oranla çok düşüktür.
- Güvenlik araçlarını kullanmak zor değildir ve kullanımları önemlidir.

Katılımcılar sadece siber saldırıların maliyetlerinin değil, siber güvenliğe akıllıca yatırım yapmanın önemini de öğrenir.

KASPERSKY lab