İşNet Oltalama Hizmeti

Saldırılar İnsan Faktörü ile Başlar, Savunma da İnsanla Şekillenir!

Saldırganlar kurbanlarını manipüle ederek şifre, kart bilgisi, kimlik bilgisi veya kurumsal erişim bilgilerini ele geçirmeye ve maddi kazanç elde etmeye çalıştığı sosyal mühendislik yöntemi en sık kullanılan ilk üç saldırı vektöründen biridir.

Saldırılar yalnızca bir e-postayla veya mesajla başlıyor ve çoğu zaman dakikalar içerisinde sonuç veriyor. İşNet Oltalama Hizmeti, kurumların en zayıf halkası olarak görünen insan faktörünü güçlendirmeye odaklanan, farkındalığı artırmaya yönelik bir güvenlik çözümüdür.

Kurumunuzu hedef alabilecek sosyal mühendislik saldırılarına karşı;

- Çalışan davranışları test edilir,
- Farkındalık seviyesi ölçülür,
- Gelişim noktaları görünür kılınır,
- Ölçülebilir güvenlik metrikleri sağlanır.

Bu sayede veri ihlallerinde en kritik saldırı yöntemlerinden biri olarak karşımıza çıkan sosyal mühendislik saldırılarına karşı davranışsal güvenlik riskleri azaltılır, kurumunuzun zafiyet oranları düşer. Yaşanabilecek maddi ve manevi kayıpların önüne geçilir.

2025 Yılında Siber Saldırılarda En Sık Görülen Sosyal Mühendislik Yöntemleri

1- Phishing (Kimlik Avı)
Kurum çalışanlarını kandırmanın bir numaralı yolu olarak kullanılıyor.

2- Pretexting (Senaryo Kurma)
Saldırganlar “banka çalışanı”, “yönetici”, “tedarikçi temsilcisi” gibi rollerle güven kazanıyor.

3- Prompt Bombing (MFA Bombardımanı)
Yeni ama hızla büyüyen bir trend. Kullanıcıya çok sayıda MFA isteği gönderiliyor ve kullanıcı bu isteklerden kurtulmak için onaylıyor.

4- Baiting (Yemleme)
SEO manipülasyonu veya sahte reklamlarla, kullanıcılar farkında olmadan zararlı yazılımları indiriyor.

İşNet Oltalama Hizmeti

Saldırılar İnsan Faktörü ile Başlar,
Savunma da İnsanla Şekillenir!

Neden İşNet Oltalama Hizmetini Tercih Etmelisiniz?

Gerçek Risklerin Ortaya Çıkarılması
Saldırganların kullandığı sosyal mühendislik teknikleri uygulanarak, kurum içerisindeki zayıf noktalar tespit edilir. Tahmin yerine ölçülebilir veriler elde edilir.

Üst Yönetim İçin Somut ve İzlenebilir Metrikler
Yönetim ekipleri için açık, anlaşılır ve karar destekleyici raporlar ile güvenlik yatırımlarının karşılığı görünür hale getirilir.

Bilgi Güvenliği Kültürü
Saldırganların kullandığı gerçekçi senaryolar üzerinden yapılan simülasyonlar, çalışan davranışlarını kalıcı olarak değiştirir ve kurum kültürünün bir parçasına dönüştürür.

İşNet Güvencesi
İşNet olarak 25 yıllık tecrübemiz ve konusunda uzman teknik insan kaynaklarımız ile sizlere uzmanlık, deneyim ve operasyonel güç kazandırıyoruz.

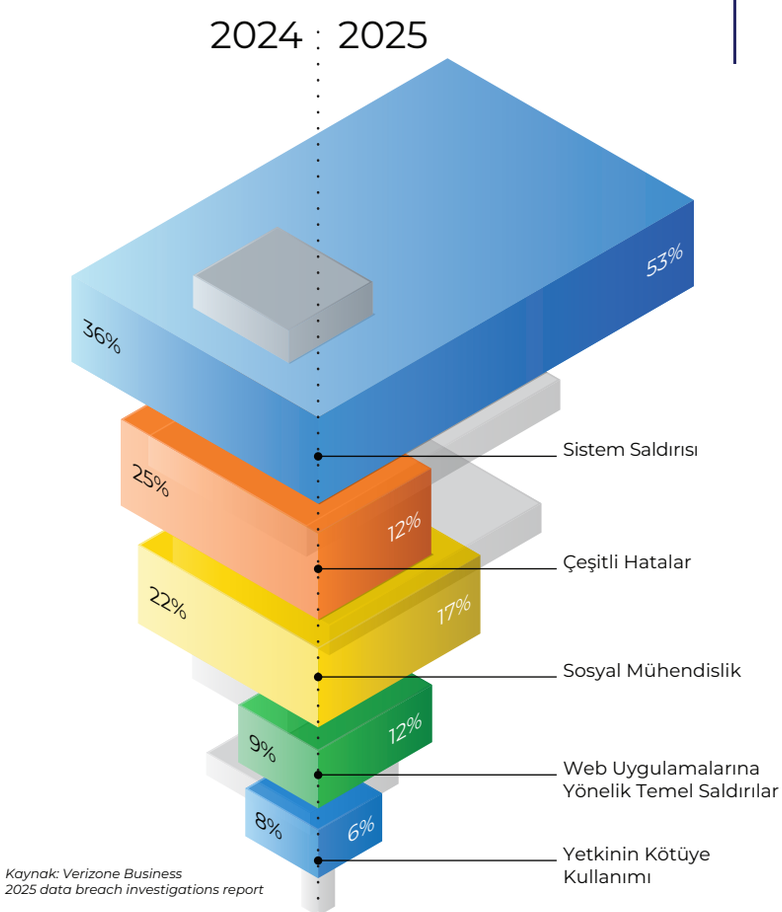
İnsan Faktörünün Siber Güvenliğin Önemli Bir Parçası Haline Getirilmesi
Kurum çalışanları olası bir saldırı anında nasıl davranmalarını gerektiğini deneyimleyerek öğrenir. Davranış temelli farkındalık kazandırılır.

Regülasyonlara Uyum
ISO 270001, KVKK, PCI-DSS gibi standartlar için gerekli olan farkındalık ve izleme faaliyetleri belgelenir ve sürdürülebilir hale getirilir.

Kurumsal Güvenin ve İtibarın Güçlemesi
Veri ihlali yalnızca maddi kayıpla sonuçlanmaz; müşteri güveni, marka itibarı ve iş ortaklıkları ciddi zarar görür. Bu hizmet ile çalışan farkındalığını yükselterek veri ihlallerinin en sık görülen nedenini ortadan kaldırılır ve şirket güvenilirliği artırılır.

Hizmet Bileşenleri

- Kurumunuza özel gerçekçi senaryolar
- Özelleştirilmiş şablon tasarımları
- Yönetilen simülasyon süreçleri
- Eğitim ve farkındalık içerikleri
- Raporlama



Kaynak: Verizone Business 2025 data breach investigations report

Sıklık

Meydana gelen **4.009** olayın **3.405**'inde doğrulanmış veri sızıntısı bulunmaktadır.

Tehdit Eden Saldırganlar

%100
Harici kaynaklı ihlaller

Saldırganların Motivasyonları

%55
Finansal kazanç

%52
Casusluk

Ele Geçirilen Veriler

%68
Dahili Veriler

%58
Diğer

%53
Gizli bilgiler