TSPB | TÜRKİYE SERMAYE PİYASALARI BİRLİĞİ

Siber Güvenlik

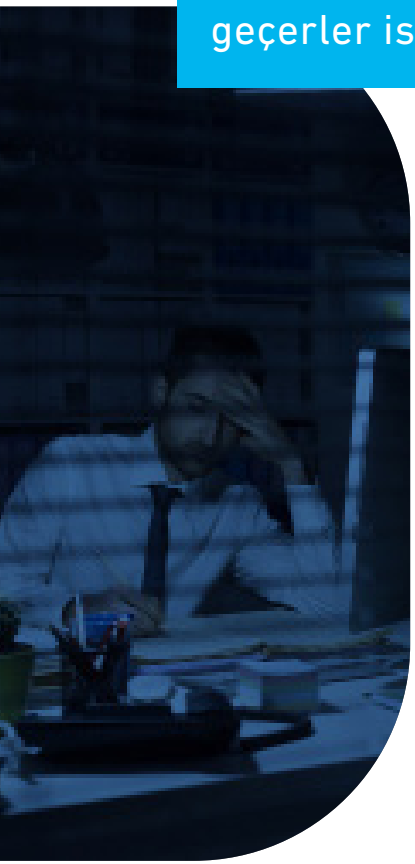
WWW.TSPB.ORG.TR

Sosyal Mühendislik ve Oltalama Nedir?

Sahte e-postalar, kullanıcıların korku, heyecan ve sevinç duygularının sömürülerek e-posta içeriğindeki linke tıklatmak ve/veya kullanıcı bilgilerini çalmak amacıyla gönderilen e-postalardır.

Sosyal Mühendislik Nasıl Yapılır?

Tehdit aktörleri sizler ile sözlü iletişime geçerler ise asağıdakiler gibi davranabilirler;



- Yetkili bir kişi (banka personeli, polis, hâkim, savcı v.b.) gibi davranarak kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.
- Kredi kartı aidatı, kredi başvuru ücreti ya da sigorta ücretinizi iade etmek için aradıklarını söyleyip kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.
- Yetkili kurumların adını vererek "Hesabınızdan adınızla izinsiz işlem yapıldı!" şeklinde yönlendirebilir ve dolandırmaya çalışabilirler.
- Covid-19 temasını kullanarak, aşı randevusu ya da "Pozitif sonuca sahipsiniz!" şeklinde kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.
- "Hediye çeki kazandınız!" ya da "Çekiliş kazandınız!" gibi heyecan yaratabilecek unsurları kullanabilir, kişisel bilgilerinizi paylaşmanızı isteyebilirler.

Sosyal Mühendislik internet üzerinden e-posta ile yapılması da mümkündür.

Güvenilir kurumlardan gönderiyormuş izlenimi yaratılarak e-posta içerikleri taklit edilebilir kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.

E-posta içeriklerinde zararlı yazılım ve aktivite oluşturabilecek dosyalar iletebilirler. Bu dosyalar “.pdf”, “.docx” ya da “.xls” uzantılı bile olabilir.

Sahte SMS ile yönlendirme yapabilirler. Farklı kurumların altyapılarını sömürerek ve kullanarak izinsiz SMS atabilirler. SMS üzerinden kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.

Sosyal medyayı kullanarak tuzak siteler ve kampanyalar oluşturabilirler.

Sosyal Mühendislikten Korunmak için Nelere Dikkat Edilmelidir?

- Kimliğinden emin olunmayan kişiler ile telefon ya da e-posta yolu ile bilgi paylaşılmamalıdır.
- Şüphelenilen e-postalara cevap verilmemeli hatta açılmamalıdır.
- E-posta yolu ile gelen dosyalar taranmadan açılmamalıdır.
- E-posta bağlantılarına erişirken dikkatli olunmalı ve kaynak kontrolü yapılmalıdır.
- Kendisini yetkili bir kişi veya kuruluş olarak tanıtan kişilere dikkat edilmelidir.

Güvende kalmak için;

- Mobil cihazlarınızı ve internet tarayıcınızı sürekli olarak güncel tutunuz.
- Sıkça işlem yaptığınız mobil uygulama ve masaüstü uygulamaların güncel olduğundan emin olunuz.
- Sosyal medya ve e-posta ile gelen güvenilir olmayan bağlantılara tıklamayınız.
- Parolalarınızı paylaşmayınız ve sürekli değiştiriniz. Çok hesap-ortak parola mantığını kullanmayınız.
- En az 8 karakter uzunluğunda; harf, sayı ve özel karakter içeren parolalar belirleyiniz.
- Mümkünse 2 aşamalı doğrulama destekleyen uygulamalar kullanınız. Pasif durumda ise aktifleştiriniz.

DLP (Data Loss Prevention - Veri Kaybı Önleme) Sistemlerinizde Önlem Alın!

Veri Kaybını Önleme (DLP) çözümleri; veri ihlallerini, sızıntıları veya hassas verilerin istenmeyen şekilde dışarı çıkartılmasını tespit etme ve önleme uygulamasıdır.

DLP çözümünüz varsa Data Discovery ve OCR kabiliyetlerini etkin bir şekilde kullandığınızdan emin olunuz. Sadece loglama için değil bloklamak için de tanımlamalar yapıldığından emin olunuz. Regex ve/veya anahtar kelimeler ile gerekli veri şablonların oluşturulduğundan emin olunuz.

Antivirüs Sistemlerinizde Önlem Alın!

Antivirüs yazılımı kötü amaçlı yazılımları engellemek, tespit etmek ve devre dışı bırakmak amacıyla kullanılan uç nokta bilgisayar programlarıdır. Amacına uygun ve faydalı bir şekilde kullanılması için;

Ürünün en stabil şekilde kullanılabilmesi için üretici tarafından yayınlanmış olan güncel sürümlerin yüklü olduğundan emin olun.

Merkezi bir sistem üzerinden yönetilebildiğinden emin olun.

Geleneksel bir yöntemin aksine, güncel teknolojileri kullanan yeni nesil bir antivirüs olduğundan emin olun.

Kurulu olmayan sistemlerin keşfi için süreç ve prosedür oluşturun ve ivedilikle kurulumları tamamlayın.

Firewall (Güvenlik Duvarı) Çözümünüzde Önlem Alın!

Firewall güvenlik mimarisinin en önemli çözümlerinden bir tanesidir. Güvenlik duvarları yani firewall sistemleri, gelen ve giden tüm ağ trafiğini kontrol ederek belirli filtrelerden geçirip, ağ trafiği içerisindeki zararlı eylemleri durdurmayı amaçlar. Amacına uygun ve faydalı bir şekilde kullanılması için;

Ürünün en stabil şekilde kullanılabilmesi için üretici tarafından yayınlanmış olan güncel sürümlerin yüklü olduğundan emin olun.

Mümkünse yedekli çalıştığından emin olun.

Güvenlik cihazı üzerinde sonlandırılmış olan VPN kullanıcılarının tanımlı olan kuralları için departman bazında gruplar oluşturulup, kuralları bu gruplara göre tanımlayın.

Arayüzler için güvenlik seviyelerini doğru şekilde konfigürasyon edin.

FQDN tanımlarında olası bir DNS server problemine karşı servis kesintisini önlemek adına ikincil DNS sunucusu tanımlayın.

Problem ve geriye dönük analizler için güvenlik duvarı üzerinde oluşan logları, harici bir kaynağa aktarın.

Firewall üzerinde bulunan arayüzlerden geçecek trafikleri sınırlamak ve ayrıştırmak için oluşturulmuş hizmet politikası tanımları kullanın.

Periyodik aralıklarla kurallar kontrol edilip, kullanılmayan ve hit almayan kurallar silinip, herhangi bir parametre bulunan kuralların güncellendiginden emin olun.

TSPB | TÜRKİYE SERMAYE PİYASALARI BİRLİĞİ

www.tspb.org.tr

tspborgtr

tspbkanali

Siber Güvenlik

Sosyal Mühendislik ve Oltalama Nedir?

Sahte e-postalar, kullanıcıların korku, heyecan ve sevinç duygularını sömürerek e-posta içeriğindeki linke tıklamak ve/veya kullanıcı bilgilerini çalmak amacıyla gönderilen e-postalardır.

Sosyal Mühendislik Nasıl Yapılır?

Tehdit aktörleri sizler ile sözlü iletişime geçerler ise aşağıdakiler gibi davranabilirler;

- Yetkili bir kişi (banka personeli, polis, hâkim, savcı v.b.) gibi davranarak kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.
- Kredi kartı aidatı, kredi başvuru ücreti ya da sigorta ücretinizi iade etmek için aradıklarını söyleyip kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.
- Yetkili kurumların adını vererek "Hesabınızdan adınızla izinsiz işlem yapıldı!" şeklinde yönlendirebilir ve dolandırmaya çalışabilirler.
- Covid-19 temasını kullanarak, aşı randevusu ya da "Pozitif sonuca sahipsiniz!" şeklinde kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.
- "Hediye çeki kazandınız!" ya da "Çekiliş kazandınız!" gibi heyecan yaratabilecek unsurları kullanabilir, kişisel bilgilerinizi paylaşmanızı isteyebilirler.

Sosyal Mühendisliğin internet üzerinden e-posta ile yapılması da mümkündür.

- Güvenilir kurumlardan gönderiyormuş izlenimi yaratılarak e-posta içerikleri taklit edilebilir kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.
- E-posta içeriklerinde zararlı yazılım ve aktivite oluşturabilecek dosyalar iletebilirler. Bu dosyalar ".pdf", ".docx" ya da ".xls" uzantılı bile olabilir.
- Sahte SMS ile yönlendirme yapabilirler. Farklı kurumların altyapılarını sömürerek ve kullanarak izinsiz SMS atabilirler. SMS üzerinden kişisel bilgilerinizi ya da parolanızı paylaşmanızı isteyebilirler.
- Sosyal medyayı kullanarak tuzak siteler ve kampanyalar oluşturabilirler.

Sosyal Mühendislikten Korunmak için Nelere Dikkat Edilmelidir?

- Kimliğinden emin olunmayan kişiler ile telefon ya da e-posta yolu ile bilgi paylaşılmamalıdır.
- Şüphelenilen e-postalara cevap verilmemeli, hatta açılmamalıdır.
- E-posta yolu ile gelen dosyalar taranmadan açılmamalıdır.
- E-posta bağlantılarına erişirken dikkatli olunmalı ve kaynak kontrolü yapılmalıdır.
- Kendisini yetkili bir kişi veya kuruluş olarak tanıtan kişilere dikkat edilmelidir.

Güvende kalmak için;

- Mobil cihazlarınızı ve internet tarayıcınızı sürekli olarak güncel tutunuz.
- Sıkça işlem yaptığınız mobil uygulama ve masaüstü uygulamaların güncel olduğundan emin olunuz.
- Sosyal medya ve e-posta ile gelen güvenilir olmayan bağlantılara tıklamayınız.
- Parolalarınızı paylaşmayınız ve sürekli değiştiriniz. Çok hesap-ortak parola mantığını kullanmayınız.
- En az 8 karakter uzunluğunda; harf, sayı ve özel karakter içeren parolalar belirleyiniz.
- Mümkünse 2 aşamalı doğrulama destekleyen uygulamalar kullanınız. Pasif durumda ise aktifleştiriniz.

TSPB | TÜRKİYE SERMAYE PİYASALARI BİRLİĞİ

DLP (Data Loss Prevention- Veri Kaybı Önleme) Sistemlerinizde Önlem Alın!

Veri Kaybını Önleme (DLP) çözümleri; veri ihlallerini, sızıntıları veya hassas verilerin istenmeyen şekilde dışarı çıkartılmasını tespit etme ve önleme uygulamasıdır.

DLP çözümünüz varsa Data Discovery ve OCR kabiliyetlerini etkin bir şekilde kullandığınızdan emin olunuz. Sadece loglama için değil bloklamak için de tanımlamalar yapıldığından emin olunuz. Regex ve/veya anahtar kelimeler ile gerekli veri şablonların oluşturduğundan emin olunuz.

Antivirüs Sistemlerinizde Önlem Alın!

Antivirüs yazılımı kötü amaçlı yazılımları engellemek, tespit etmek ve devre dışı bırakmak amacıyla kullanılan uç nokta bilgisayar programlarıdır. Amacına uygun ve faydalı bir şekilde kullanılması için;

- Ürünün en stabil şekilde kullanılabilmesi için üretici tarafından yayınlanmış olan güncel sürümlerin yüklü olduğundan emin olun.
- Merkezi bir sistem üzerinden yönetilebildiğinden emin olun.
- Geleneksel bir yöntemin aksine, güncel teknolojileri kullanan yeni nesil bir antivirüs olduğundan emin olun.
- Kurulu olmayan sistemlerin keşfi için süreç ve prosedür oluşturun ve ivedilikle kurulumları tamamlayın.

Firewall (Güvenlik Duvarı) Çözümünüzde Önlem Alın!

Firewall güvenlik mimarisinin en önemli çözümlerinden bir tanesidir. Güvenlik duvarları yani firewall sistemleri, gelen ve giden tüm ağ trafiğini kontrol ederek belirli filtrelerden geçirip, ağ trafiği içerisindeki zararlı eylemleri durdurmayı amaçlar. Amacına uygun ve faydalı bir şekilde kullanılması için;

- Ürünün en stabil şekilde kullanılabilmesi için üretici tarafından yayınlanmış olan güncel sürümlerin yüklü olduğundan emin olun.
- FQDN tanımlarında olası bir DNS sunucu problemine karşı servis kesintisini önlemek adına ikincil DNS sunucusu tanımlayın.
- Güvenlik cihazı üzerinde sonlandırılmış olan VPN kullanıcılarının tanımlı olan kuralları için departman bazında gruplar oluşturup, kuralları bu gruplara göre tanımlayın.
- Mümkünse yedekli çalıştığından emin olun.
- Arayüzler için güvenlik seviyelerini doğru şekilde konfigürasyon edin.
- Problem ve geriye dönük analizler için güvenlik duvarı üzerinde oluşan logları harici bir kaynağa aktarın.
- Firewall üzerinde bulunan arayüzlerden geçecek trafikleri sınırlamak ve ayrıştırmak için oluşturulmuş hizmet politikası tanımları kullanın.

Periyodik aralıklarla kurallar kontrol edilip, kullanılmayan ve hit almayan kurallar silinip, herhangi bir parametre bulunan kuralların güncellendiğinden emin olun.