Siber Teröristlere Karşı Kurumlar Nasıl Korunmalıdır?

Yusuf TULGAR

NetDataSoft Genel Müdürü

email: yusuf@netdatasoft.com

Siber Teröristlerin Amaçları

- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme
- Bilgisayar Sabotajı
- Bilgisayar Yoluyla Dolandırıcılık
- Bilgisayar Yoluyla Sahtecilik
- Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı
- Yasadışı Yayınlar
- Servisi Durdurmak
- Kurum Dışına Bilgi Sızdırmak
- İdeolojik Eylemler
- İçeri Zararlı Uygulama Yerleştirerek Ajanlık Yapmak
- Kurum Verilerini Silmek, Bozmak, Yok Etmek
- Kurum Verileri İle Tehtid, Şantaj ve Haksız Yere Kazanç Sağlamaya Çalışmak

Siber Saldırılarda Kurumlarda Oluşabilecek Güvenlik Zafiyetleri

- Kurum uygulamaları aracılığı ile belirli bir olay, zaman veya dışarıdan müdahale durumlarında, kurum içerisinden kurum dışarısına bilgi sızdırmasını önlemek amacıyla tüm uygulamaların kullandıkları portlar izlenmeli, veri trafiği engellenmeli ve tüm hareketler loglanmalıdır.
- Kurum bilgi sistemleri üzerinde gerçekleşen tüm bilgi akışı faaliyetleri izlenerek merkezi olarak loglanmalıdır.
- Kurumsal ağa dahil olan tüm cihazlar merkezi olarak yetkilendirilmelidir. Yetkilendirilmeyen cihazların kurum ağına erişimleri yasaklanmalıdır.
- Kurum içerisindeki tüm verilerin %100 kurumda kalması sağlanmalı ve tüm erişim faaliyetleri loglanmalıdır.
- Kurum verilerinin tüm erişimleri yetkilere bağlanmalıdır. Yetkisiz kişilerin başkalarının verilerine erişimleri engellenmelidir.
- Kurumdaki tüm sistemlerin event logları toplanmalı, dinlenmeli, saklanmalı ve analiz edilmelidir.
- Tüm kurum verileri kriptolanarak saklanmalı ve sadece ilgilisinin erişimine izin verilmelidir.

Kurum Verilerinin Yetkisiz Kişilerce Kurum Dışına Çıkartma Yöntemleri

- Kurum verileri temelde 3 yoldan yetkisiz kişilerde kurum dışına çıkartılabilir.

1. **Fiziksel Olarak Veriyi Kurum Dışına Çıkartmak**
    1. Kurum bilgileri yazıcı çıktısı alınarak
    2. Verilerin USB belleklere ve taşınır disklere kaydı yapılarak
    3. File Sistemlerdeki dosyalara kaynağından 1e 1 kopyalayarak
2. **Ağ Üzerinden Veriyi Kurum Dışına Çıkartmak**
    1. FTP, Gmail, Hotmail, WeTranfser vb. yabancı menşeli sistemler üzerinden
    2. Kurum dışından erişimi olan WI-FI kablosuz ağ üzerinden
    3. Kullanıcı adı ve şifresi hırsızların eline geçmiş kurumun dışa açık güvenli hattı üzerinden
3. **Kurumda Çalışan Uygulamaların Arka Kapı (BackDoor) Üzerinden Veriyi Kurum Dışına Çıkartmak**
    1. Mesajlaşma uygulamaları kullanılarak verilerin mesaj şeklinde dışarı çıkartılması.(WhatsApp vb)
    2. Kurumsal Email kullanılarak verilerin dışarı çıkartılması
    3. Uygulamanın dışarıdaki bir casus uygulama veya servis ile bire bir - bir bağlantı sağlayarak verileri dışarıya çıkartması

Kurumsal Dijital Arşiv Güvenliği

- Kurumlara önceden alınmış ve aktif kullanılan uygulamaların gerekli sızma testi ve kod incelemeleri yapılmadan hala kullanılıyor olması, kurum verilerinin güvenliği açısından büyük risk taşımaktadır.
- Kurumlarımızda alınacak her türlü güvenlik önlemlerine rağmen göz ardı edilen veya tespit edilemeyen bir açıklıktan dolayı kurum içerisine kötü niyetli kişi ve sistemlerin sızması, olası bir durumdur. Böyle bir sızma durumunda kötü niyetli yazılımlar ve kişiler tüm kurum verisini rahatlıkla dışarı sızdırabilir.
- Dünya genelinde bir çok arşiv sistemi 256 bitlik kripto kullanır ve henüz kırılamamıştır. Eğer kurum verileri kriptolanmadan arşivlenirse, kolaylıkla tüm veriler çalınarak kurum dışına çıkartılabilir. Bu yüzden kurumun sahip olduğu tüm dijital ortamdaki veriler **512 bit kriptolu** bir şekilde arşivlenmelidir. Bu şekilde arşivlenen hiçbir kurum verisi yetkisiz ve izinsiz kişi, sistem ve yazılımlar aracılığıyla anlamlandırılamaz, çalınamaz ve kopyalanamaz.

Siber Saldırılarda Alınması Gereken Tedbirler ve Savunma Yöntemleri

- E-Posta Güvenlik Tedbirleri
- Şifre Güvenlik Tedbirleri
- Anti-Virüs Güvenlik Tedbirleri
- Sunucu Güvenlik Tedbirleri
- Ağ Yönetimi Tedbirleri
- Kablosuz İletişim Tedbirleri
- Kriz ve Acil Durum Yönetimi Tedbirleri
- Kimlik Doğrulama ve Yetkilendirme Tedbirleri
- Veri Tabanı Güvenlik Tedbirleri
- Yazılım Geliştirme Tedbirleri

Kurumlarda Güvenlik için 20 Kritik Kontrol

- Donanım Envanteri
- Yazılım Envanteri
- Mobil Cihazlar, dizüstü bilgisayarlar, iş istasyonları ve Sunucuların Donanım ve Yazılımlarının Güvenli bir şekilde Yapılandırılmaları
- Ağ Donanımları Kontrolü
- Zararlı Yazılımlara (Malware) Karşı Savunma
- Uygulama Yazılımlarının Güvenliği
- Kablosuz Erişim Denetimi
- Veri Kurtarma Kapasitesi
- Güvenlik Becerilerini Değerlendirme ve Uygun Eğitimler ile Zafiyet olan Alanları Giderme
- Güvenlik Duvarları, Router ve Switch gibi Ağ cihazlarının Güvenli bir şekilde yapılandırılmaları

Kurumlarda Güvenlik için 20 Kritik Kontrol

- Ağ Bağlantı Noktaları (Port), Protokoller ve Servislerin Kontrolü
- Sistem Yönetici Yetkilerinin Kontrolü
- Sınır Savunma
- Logların Güvenli Olarak Kaydedilmesi, Yönetilmesi Ve İzlenmesi
- Güvenlik Eğitimleri
- Kullanıcı Hesabı Denetimi
- Veri Koruma
- Bilgisayar Olaylarına Müdahale
- Güvenli Ağ Mühendisliği
- Güvenlik Analizi ve Sızma(Penetration) Testleri