T.C.
CUMHURBAŞKANLIĞI
Dijital Dönüşüm Ofisi Başkanlığı
Siber Güvenlik Dairesi Başkanlığı

Ek-2

TÜRKİYE CUMHURİYETİ'NİN YÜZÜNCÜ YILI

ACELE

Sayı : E-35030449-719-14132
Konu : E-Posta Güvenliği

DAĞITIM YERLERİNE

Günümüzde bilgi teknolojilerinin gelişmesi ve dijitalleşmenin artmasıyla beraber siber tehditler daha karmaşık, hedef odaklı ve kalıcı hale gelmiş; devlet destekli siber operasyonların sayısı artış göstermiştir.

Bilişim sistemlerine, kritik altyapı ve veriye yönelik gerçekleştirilen siber saldırılar ülke ekonomisi ile kamu düzenine zarar vermekte ve sonuç olarak milli güvenliği tehdit etmektedir. Nitekim, Rusya-Ukrayna savaşında konvansiyonel savaş yöntemlerine devlet kurumları ve kritik altyapıya yönelik siber saldırılar da eşlik etmiştir. Siber savaşa siber tehdit grupları da dahil olmuş; Rusya ve Ukrayna'nın yanı sıra taraflara destek veren ülkelere yönelik de siber operasyonlar yürütülmüştür. Devam eden İsrail-Hamas çatışmasının da siber operasyonlar ile desteklenmesi ve bu operasyonlarda ülkemizin hedef alınması ihtimaller dahilindedir.

Kamu kurumları ve kritik önemi haiz kuruluşlara ait e-posta sistemleri, önemli veri ve yazışmaları barındırmasının yanı sıra "oltalama" yöntemiyle zararlı yazılım dağıtımında da kullanılmaları sebebiyle tehdit gruplarının en önemli hedefleri arasında yer almaktadır. Ayrıca yapay zeka destekli sosyal mühendislik yöntemlerinin söz konusu oltalama saldırılarının ikna ediciliğini artırmada yaygın olarak kullanıldığı müşahede edilmektedir. Bu nedenle, kamu kurumlarına ait e-posta sunucularının doğru yapılandırılması ve gerekli güvenlik tedbirlerinin alınması önem arz etmektedir.

Bu kapsamda;

- E-posta hesaplarında güçlü ve benzersiz parolaların kullanılması, en fazla üç ayda bir kullanıcıların parolalarını değiştirmeye zorlanmaları,
- E-posta sunucularına kurum ağı dışından erişim sırasında çift kademeli kimlik doğrulamasının (kullanıcı mobil cihazına tek kullanımlık şifre gönderimi vb.) uygulanması,
- Oturum açma ekranlarında ardışık şifre deneme saldırılarının önüne geçilebilmesi amacıyla insan ve makine ayrımı yapan tekil resim doğrulaması (captcha) veya farklı türdeki erişim kontrol metotlarının uygulanması,
- Kurumun e-posta sunucularının web erişimlerinin yurt dışına kapatılması; yurt dışından erişim gerektiğinde e-posta sunucusunun internet erişim ara yüzüne sadece kurumsal sanal özel ağ (VPN) kullanılarak erişilmesi,

Cumhurbaşkanlığı Çankaya Yerleşkesi, Ziaur Rahman Caddesi 06550 Çankaya / Ankara/ Türkiye
Tel: 0 312 969 3900 0 312 969 3901
KEP Adresi : cbddo@hs01.kep.tr

Ek-2

- E-posta sunucularına yalnızca tanımlanmış cihazlardan erişime izin verilmesi,
- Gönderen Politikası Çerçevesi (Sender Policy Framework-SPF) ve Alan Adı Anahtarıyla E-posta Doğrulama (Domain Keys Identified Mail-DKIM) kayıtlarının alan adı sistemine (Domain Name System-DNS) eklenmesi ile e-postaların gönderildiği kaynakların doğrulanması,
- Kötüye kullanım ve olası siber saldırı oluşması durumunda teknik incelemelerin gerçekleştirilebilmesi amacıyla e-posta sisteminde etkili bir log mekanizmasının işletilmesi,
- E-posta sunucusu ile istemcisi arasındaki iletişimde kimlik doğrulama ve veri iletimi için TLS kullanımının zorunlu olacak şekilde yapılandırılması,
- Kuruma dışarıdan gelen e-posta eklerinin çok katmanlı güvenlik analizinden (içerik analizi, beyaz liste/kara liste, imza tabanlı anti-virüs, anti-malware taramaları vb.) geçirilmesi; bu analizler neticesinde kategorilendirilmemiş e-posta eklerinin kum havuzunda (sandbox) çalıştırılması,
- Kurumsal e-posta hesaplarının bankacılık, alışveriş vb. iş dışı faaliyetlerde kullanılmaması için personelin bilinçlendirilmesi,

önlemlerinin tüm kamu kurum ve kuruluşları tarafından uygulanması gerekmektedir.

İlaveten, ülkemizin siber güvenliğinin artırılması için başta Ek'te yer alan e-posta sunucularına yönelik güvenlik tedbirleri olmak üzere Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan ve "cbddo.gov.tr/bigrehber/" adresinde yer alan Bilgi ve İletişim Güvenliği Rehberindeki siber güvenlik tedbirlerinin alınmasında fayda mütalaa edilmektedir.

Kurum ve kuruluşlarca, bağlı/ilgili/ilişkili kurum ve kuruluşlarına dağıtımının yapılması hususunda bilgilerinizi ve gereğini arz/rica ederim.

Yusuf TANCAN
Başkan a.
Siber Güvenlik Dairesi Başkanı

Ek: E-Posta Güvenliği (3 Sayfa)

Dağıtım:
Dağıtım Listesi (57 Muhatap)

Cumhurbaşkanlığı Çankaya Yerleşkesi, Ziaur Rahman Caddesi 06550 Çankaya / Ankara/ Türkiye
Tel: 0 312 969 3900 0 312 969 3901
KEP Adresi : cbddo@hs01.kep.tr

Ek-2

DAĞITIM LİSTESİ

Gereği:

Tüm Kamu Kurum ve Kuruluşlarına
Düzenleyici ve Denetleyici Kurum ve Kuruluşlara
Türksat Uydu Haberleşme Kablo Tv ve İşletme Anonim Şirketi Genel Müdürlüğüne
TÜRK TELEKOM A.Ş 'NE
TURKCELL İLETİŞİM HİZMETLERİ A.Ş.'NE
VODAFONE TELEKOMÜNİKASYON A.Ş 'NE

Bilgi:

Cumhurbaşkanlığı İdari İşler Başkanlığına
Milli İstihbarat Teşkilatı Başkanlığına

Cumhurbaşkanlığı Çankaya Yerleşkesi, Ziaur Rahman Caddesi 06550 Çankaya / Ankara/ Türkiye
Tel: 0 312 969 3900 0 312 969 3901
KEP Adresi : cbddo@hs01.kep.tr