BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

23.04.2020


**Bilgi Teknolojileri ve İletişim Kurumu (BTK)**
**Ulusal Siber Olaylara Müdahale Merkezi (USOM)**
**Adres:** Bilgi Teknolojileri ve İletişim Kurumu (BTK) Merkez Binası
Eskişehir Yolu 10.Km No:276 Çankaya/Ankara
**Telefon Numarası:** +90 312 586 53 05 - 0549 779 87 85
**Fax:** +90 312 586 54 00
**iletisim@usom.gov.tr**

# UZAKTAN ERİŞİM SERVİSLERİNE YÖNELİK ÖNLEMLER

SÜRÜM 1.0

ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ

Ülkemiz ve tüm dünyanın içinde bulunduğu COVID-19 salgını döneminde uzaktan çalışma yöntemi kullanan kamu kurum ve kuruluşları, özel sektör ve çalışanlar için dikkat edilmesi gereken genel hususlar, alınması gereken tedbirler ve uyulması gereken kurallar USOM tarafından yayınlanan **TR-20-159 (Güvenli "Uzaktan Çalışma" Kuralları)** güvenlik bildirimi ile duyurulmuş ve aşağıda hususlar sıralanmıştır.

## 1. TR-20-159 :Güvenli "Uzaktan Çalışma" Kuralları

### Uzaktan çalışma yöntemini uygulayan kurumlar ve sistem yöneticileri tarafından;

1. Güvenlik ve çalışma koşullarına ilişkin risklerin belirlenmesi ve minimize edilerek uzaktan çalışma koşullarının oluşturulması için teknik ve idari personelin içinde bulunduğu bir çalışma grubunun oluşturulması önem arz etmektedir.
2. Uzaktan erişime açılamayacak derecede kritik hizmetlerin risk değerlendirmelerinin yapılması gerekmektedir. Uzaktan erişime uygun olmayan kritik hizmetler ve kaynaklar için önceliklendirme yapılması, yeterli sayıda personelin yedekli biçimde iş yerinde bulundurulması ve görevlendirilmesi sağlanmalıdır.
3. Uzaktan çalışan tüm personele özellikle güçlü parola kullanımı, sosyal mühendislik saldırıları ve güvenlik yazılımları hakkında farkındalık eğitimi verilmeli ve oryantasyon yapılmalıdır.
4. Uzaktan erişim için VPN veya uzaktan yönetim servisi (RDP, SSH vb.) kullanılması durumunda;
    - İlgili sistemlerin en güncel/stabil/güvenli versiyonu kullanılmalıdır.
    - Sistemlerin desteklediği tüm güvenlik önlemleri doğru ve tam şekilde yapılandırılmalıdır.
    - Üretilen iz kayıtları (logların) olası bir saldırıyı tespit edecek şekilde düzenli olarak kayıt altına alınmalı,
    - Yetkisiz erişim, kaba kuvvet (brute force) saldırıları vb. anomalilerin tespiti için alarm mekanizmaları oluşturulmalıdır.
    - Yetkiler "en az gerekli yetki" (least privileged access) prensibine uygun verilmelidir.
    - Sistemler üzerinde maksimum bağlantı süresi için bir zaman aşımı tanımlanmalıdır.
    - Uzaktan çalışma boyunca tanımlanan kurallar geçici süreliğine oluşturulmalıdır.
    - Mümkün olduğu durumlarda uzaktan bağlantılar için "kaynak IP" kısıtlaması yapılmalıdır.
5. Erişimler için çok faktörlü kimlik doğrulama ve zaman bazlı yetkilendirme önlemleri alınmalıdır.
6. Uzaktan çalışan personel için güvenlik önlemleri alınmış sistemler/bilgisayarlar verilmesi gerekmektedir.
7. Risk değerlendirmesine göre uzaktan erişimin tanımlanmaması gereken hiçbir kritik sisteme erişim için izni verilmediğinden emin olunması gerekmektedir.

**Uzaktan çalışan personel tarafından;**

1. Uzaktan çalışma için kullanılan sistemlerde (PC, laptop, tablet, telefon vb.) gerekli güvenlik yazılımlarının yüklendiğinden, güncel yazılımların kullanıldığından, zararlı yazılım bulunmadığından emin olunmalıdır.
2. Uzaktan çalışma sırasında dahi olsa, kurum dışına herhangi bir kritik verinin çıkarılmaması ve kaydedilmemesi gerekmektedir.
3. Dışarıya çıkarılması zorunlu, kritik olmayan verilerin, kopyalandığı veya taşındığı sistemlerin takip edilmesi, söz konusu verilerin güvenliğinin sağlanması gerekmektedir.
4. Bağlantının büyük bir çoğunluğunun kablosuz modemler ile yapılacağı varsayıldığında kablosuz modemler üzerinde WPA/WPA2 protokolünün kullanılması, Mac adresi filtreleme, SSID gizleme gibi önlemlerin alınması gerekmektedir.

## 2. Uzaktan Erişim Servislerine Yönelik Önlemler

Güvenli uzaktan çalışma kurallarına ilave olarak; kurumların, çalışanlarının kurum kaynaklarına erişebilmesi için kullandığı farklı yöntemlere ilişkin, kurum uygulamalarında güvenlik riskleri doğmaması adına **güncel zafiyetler ve ataklar çerçevesinde alınacak önlemler** aşağıda sunulmuştur.

### 2.1. VPN Erişimleri

1. Uzaktan çalışma süresince, kurum ağındaki kaynaklara erişimler, **doğrudan erişim yerine VPN cihazları üzerinden** sağlanmalıdır. **Çok faktörlü doğrulama** özellikleri devreye alınmalı ve güçlü parola politikaları uygulanmalıdır.

2. Ayrıca kullanılan VPN cihazlarının **güncel yazılım/yamalar** ile çalıştığı kontrol edilmelidir. Uzaktan çalışmalarda sıkça kullanılan ve yakın zamanda çıkan zafiyet listesi aşağıda sunulmuştur. Bu zafiyetlere sahip ağ ve güvenlik cihazlarında, kullanıcıların **parola bilgileri saldırganlarca kolayca elde edilebilir** ve/veya ilgili ağ cihazı üzerinde **uzaktan komut çalıştırma (RCE) vakaları** yaşanabilir. Bu nedenle kurumunuz tarafından kullanılan VPN amaçlı ürünlerin, öncelikli aşağıdaki listedeki zafiyetler olmak üzere yayınlanmış güvenlik zafiyetlerini yakından takip edip güncellemelerinin ve yamalarının uygulanması önerilmektedir.

   CVE-2019-11510 - TR-20-008 - Pulse Connect Secure (PCS)
   http://www.usom.gov.tr/tehdit/842.html

   CVE-2018-13379 - TR-19-068 - Fortinet SSL VPN
   https://www.usom.gov.tr/tehdit/555.html

   CVE-2019-1579 - TR-19-124 - Palo Alto Firewall/VPN
   https://www.usom.gov.tr/tehdit/832.html

CVE-2019-16701 - TR-19-175 - pfSense
https://www.usom.gov.tr/tehdit/663.html

CVE-2020-8054 - TR-20-121 - Zyxel NAS ve Firewall Cihazları
https://www.usom.gov.tr/tehdir/955.html

CVE-2020-8515 - TR-20-182 - Drytek Endüstriyel Ürünler
https://www.usom.gov.tr/tehdit/1030.html

3. Saldırganlarca yapılan erişim denemelerinin gözlemlenebilmesi için gerekli iz kayıtlarının devrede olduğuna emin olunmalıdır.

4. Kurum VPN cihazlarında **zafiyetli sürüme** sahip yazılımların bulunduğunun tespiti halinde; ivedi olarak sistem ve güvenlik cihazlarındaki log/**kayıtları geriye dönük detaylıca incelenip**, saldırganlarca bu zafiyetlerin istismar edilip edilmediği kontrol edilmelidir. Aynı şekilde mevcut kullanıcı ve parola bilgilerinin ele geçirilebildiği göz önünde bulundurularak parolalarının sıfırlanması gerekmektedir.

5. Mümkün olduğunca kullanıcılara kurum içindeki rolleri göz önünde bulundurularak **ihtiyacı olan en az yetki** verilmesi önerilmektedir. Böylelikle olası benzer zafiyetlerin çıkması ve/veya istismarı durumunda saldırıların etkisi asgari düzeye indirgenmiş olacaktır.

## 2.2. Uzaktan Yönetim Servisleri

1. Kurumların hali hazırda VPN cihazları bulunmaması durumunda özellikle örnekleri aşağıda belirtilen uzaktan yönetim servislerine internet üzerinden tüm kullanıcıların erişimine açmak yerine ilgili servislere **sadece erişmesi gereken kullanıcıların IP adreslerine** erişim izni verilerek açılması önerilmektedir.

   Telnet: 23/tcp, 2323/tcp; SSH: 22/tcp, 2222/tcp; RDP: 3389/tcp; IPMI: 623/tcp, 623/udp; VNC: 5900/tcp; SNMP: 161/udp; 161/tcp, RSH: 514/tcp; WinRM/WSMAN: 5985/tcp, 5986/tcp, 5985/udp, WMI/RPC: 135/tcp, 135/udp

2. Uzaktan yönetim servisleri arasında yaygın olarak kullanılan RDP protokolü için uzaktan komut çalıştırmaya izin veren **aşağıda belirtilen zafiyetleri gidermek adına ilgili güvenlik yamalarını**n uygulandığına emin olunmalıdır. Söz konusu zafiyetlerin APT gruplarınca hedef alındığı gözlemlenmektedir.

   CVE-2020-0609, CVE-2020-0610 - Remote Desktop Gateway (RD Gateway)
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610

   CVE-2019-0708 Remote Desktop Protocol (RDP) (Bluekeep)
   https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

3. APT gruplarınca son zamanlarda sıkça hedef alınan bir başka zafiyet ise Microsoft ürününe ait **e-posta servis yönetim servislerinde** bulunmaktadır. Bu zafiyetin istismarı için saldırganların kurum içinde en az bir kullanıcının kimlik doğrulama bilgilerine sahip olması gerekmektedir. Bu bilgiler ile kullanıcıların kendi hesaplarına ilişkin bazı ayarların yapılabildiği yönetim servisinden elde edeceği bazı anahtarlar ile **tüm e-posta altyapısı sitemleri üzerinde uzaktan komut çalıştırma** atak vektörü ile tüm **sistemlerin ele geçirilebilmesi** söz konusu olabilmektedir.

   CVE-2020-0688, CVE-2019-19781 - TR-20-135 - Exchange Admin Center
   https://www.usom.gov.tr/tehdit/969.html

   Yukarıdaki zafiyeti barındıran sistemlerde;
   i. Söz konusu Microsoft Exchange servisindeki güncellemelerin uygulanması gerekmektedir.
   ii. Söz konusu zafiyetin istismarının başladığı Exchange Control Panel (ECP) dizinin (varsayılan olarak /ecp dizini) İnternetten erişimlerinin kapatılması gerekmektedir.
   iii. İlave olarak, iç ağdan da erişimlerin kısıtlı olarak uygulanması önerilmektedir.
   iv. Sistemlerde geriye dönük kayıtlarda gerekli incelemelerin yapılarak, söz konusu zafiyetin istismarının söz konusu olup olmadığının kontrol edilmesi gerekmektedir.
   v. Mevcutta kullanılan güvenlik uygulamalarında imza tabanlı CVE-2020-0688 imzasının ivedi bir şekilde açılmasını sağlamak önem arz etmektedir.

4. Microsoft Windows ortamında kullanılan SMBv3 protokolü için uzaktan komut çalıştırmaya izin veren aşağıda belirtilen zafiyetleri gidermek adına ilgili güvenlik yamaların uygulandığından emin olunmalıdır. Söz konusu zafiyete karşın önlem alınmaması halinde "WannaCry" saldırısı ile eşit etki oluşturabilecek saldırıların gerçekleşme potansiyeli bulunmaktadır.

   CVE-2020-0796 – TR-20-142 – Microsoft SMBv3 Zafiyeti
   https://www.usom.gov.tr/tehdit/976.html
   https://www.usom.gov.tr/tehdit/977.html

## 2.3. Endüstriyel Kontrol Sistemleri

Kurumunuz tarafından Endüstriyel Kontrol Sistemleri kullanılması durumunda dikkat edilmesi gereken temel hususlar aşağıda belirtilmiştir.

1. Sadece **uzaktan çalışma süresince erişim** açmak yerine, endüstriyel kontrol sistemi bileşenleri ve haberleşme servislerinin internet erişimine sürekli olarak açık olması güvenlik riski teşkil etmektedir.
   i. Eğer ilgili servislerin internet üzerinden erişimine ihtiyaç var ise yalnızca **yetkilendirilmiş IP** adreslerin erişimine izin verilecek şekilde kısıtlama uygulanmalıdır.
   ii. İnternete **açılmaması önerilen** endüstriyel kontrol sistemi servislerine ait örnekler aşağıda paylaşılmaktadır.

Modbus/TCP: 502/tcp; DNP3: 20000/tcp; Ethernet/IP: 44818/udp; Niagara Fox: 1911,4911/tcp; IEC 60870-5-104: 2404/tcp; ATG: 10001/tcp; BACnet: 47808/udp; HART-IP: 5094,20004/udp;

2. Endüstriyel kontrol sistemi servislerine erişimde **güçlü parolalar** seçilmelidir. Parolasız veya varsayılan kullanıcı adı/parola ile olan hesaplar kapatılmalıdır. Ayrıca parolalar; kurum adı, kişi adı, uygulama adı gibi bilgiler içermemelidir.

3. Endüstriyel kontrol sistemlerine dış ağdan teknik destek veya uzaktan bağlantı yapılması gereken durumlarda üçüncü parti yazılımlar kullanılması yerine VPN altyapısının kullanılması ve uzak bağlantı sırasında ilgili personelin yapılan işleri izlemesi gerekmektedir.

4. Endüstriyel kontrol sistemlerini ve ilişkili sistemlerin dış ortamlardan ayırmak için kullanılan güvenlik duvarı yapılandırmalarında içe doğru **(inbound)** uygulanan kısıtlar gibi dışa doğru **(outbound)** da kısıt uygulanmalı, iç ağdan dışarı kontrolsüz erişim sağlanamamalıdır.

5. Kurum iç ağında kritik sistemlere erişimin etkili bir şekilde kontrol edilmesi ve kısıtlanması gerekmektedir. Gerekli izinler ‘en az yetki’ ve ‘görevlerin ayrımı’ prensipleri göz önünde bulundurularak verilmelidir.