# UZAKTAN ÇALIŞMA GÜVENLİĞİ

**HAZIRLAYAN**

**Çetin YILMAZ**

**Bilgi Güvenliği Yönetmeni**



**Kumport Liman Hizmetleri ve Lojistik San. ve Tic. A.Ş.**

**2022**

2019 yılında başlayan ve halen devam eden, özel hayatımız ile iş hayatımıza köklü değişiklikler getiren pandemi ile birlikte profesyonel iş hayatı da acilen gerçekleştirilmesi gereken değişikliklerle karşı karşıya kaldı.

Dünyadaki genelinde ortaya çıkan bu karmaşa ve panik havasını vakit geçirmeden değerlendiren siber saldırganların yaptıkları saldırılardaki artışın birçok raporda yer aldığına şahit oluyoruz. Interpol'un **Ağustos 2020** tarihli **Cybercrime:Covid-19 Impact** adlı raporundaki rakamlar bu konudaki artışı açıkça ifade etmektedir.[1]

Pandemi etkisiyle acilen uygun şartların sağlanması konusunda başı çeken uzaktan çalışma ihtiyacı sebebiyle gündelik çalışmalarında dijital bilgi kaynaklarına erişim ihtiyacı hisseden çalışan ve diğer paydaşların bu kaynaklara erişimi için uzaktan erişim teknolojilerinin kullanımı olmazsa olmaz bir ihtiyaç haline geldi.

Uzaktan erişim teknolojileri iş hayatımızda her ne kadar kolaylık sağlasa da beraberinde getirdiği güvenlik riskleri ve karşılaşılabilecek tehdit aktörlerinin sayısı artmakta, uzaktan çalışılan ortamın kurumların güvenlik denetimlerine daha az uğraması da bu oranı artırmaktadır.

Kurumların uzaktan erişim güvenliği için alması gereken önlemler her bir organizasyona özel iş süreçleri, organizasyonun sahip olduğu teknolojiler vb. birçok parametreye bağlı olsa da genel bakış açısının diğer tüm bilgi güvenliği süreçlerinde olması gerektiği gibi aşağıdaki 3 ana başlık altında toplanması gerektiğini söyleyebiliriz.



**İnsan Faktörü**

Bu başlık altında ele alınması gereken en önemli unsur uzaktan bağlantı yapan kişilerin kendi kendilerine alabilecekleri önlemleri de içerecek şekilde bilgi güvenliği farkındalığının sağlanması ve güncel tutulmasıdır.

Güvenli olmayan ağların ve cihazların kullanılmaması, kurumsal bilgi içeren ortamların (belge, PC/notebook, akıllı telefon vb.) kontrolsüz bırakılmaması, phishing vb. saldırılara karşı alınan e-postaların ve erişim yapılan web sitelerinin içeriklerinin bilgi güvenliği açısından değerlendirme becerisi, güncel siber saldırı teknikleri hakkında bilgi sahibi olma, birebir görüşmelerde veya video konferans esnasında yapılan bilgi paylaşımlarında dikkat edilmesi gereken noktalar, çevresel etkenler sebebiyle kontrol dışı gerçekleşebilecek olaylara karşı alınabilecek önlemler gibi konular bu başlık altında ele alınmalıdır.

Tabii ki sadece teknolojiyi kullanan değil bu teknolojinin kurulumundan yönetimine kadar olan süreçlerde yer alan teknik çalışmaları gerçekleştiren kişilerden kaynaklı risklerde değerlendirilmelidir.

**Teknoloji Faktörü**

Uzaktan bağlantı için kullanılan teknolojiler ve iletişim ağlarındaki riskler bu başlık altında değerlendirilebilir.

[1] https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

Kullanılan PC/notebook vb. bilgi sistemleri cihazlarının güncelliği ve merkezi yönetimi, bilginin tutulduğu ortamlara erişim de AAA[2] konseptinin doğru şekilde uygulanması ve mümkün olduğunca MFA [3]ile desteklenmesi, güvenlik cihazlarının yetenekleri, yönetimi ve güncelliği, kontrol dışı gerçekleşmesi muhtemel veri kaçaklarının izlenmesi için DLP teknolojilerinin etkin şekilde kullanılması, hesapların yönetimi için PAM ve IAM çözümlerinin kullanımı, mobil cihazların güvenliği için MDM çözümleri, uç nokta güvenliğinin sağlanması için antivirüs vb. teknolojilerin kullanımı ve güncel tutulması, anomali takibi ve olay müdahalesi için SIEM,EDR,XDR vb. teknolojilerin kullanılması, iletişim güvenliğinin sağlanmasında kriptografik kontrollerin uygulanması gibi çözümler ile ZTNA ve SASE teknolojileri bu kapsamda değerlendirilebilir.

**Süreç Faktörü**

Özellikle bilgi güvenliğinin sağlanmasına direk etki eden süreçler ve süreçlere bağlı riskler iyi değerlendirilmeli, birbirini etkileyen süreçler geliştirmeye açık ve esnek olmalı, süreçlerde yer alan paydaşların açık bir şekilde iletişimde olduğu bir süreç yönetimi ve iyileştirmesi sağlanmalıdır.

Daha etkin güvenlik yönetimi için organizasyonların uyum zorunlulukları olmasa bile CBDDO Bilgi ve İletişim Güvenliği Rehberi, ISO 27000 serisi, NIST, IMO-Guidelines on Maritime Cyber Risk Management vb. genel kabul görmüş framework ve belgeler rehber olarak değerlendirilebilir.

Sonuç olarak, uzak bağlantı güvenliği genel bilgi güvenliği prensiplerinden ayrı düşünülmemelidir. Yukarıda üç başlık altında geniş bir bakış açısı ile ele alınan hususlar organizasyonların yapılarına ve işleyişlerine göre değişiklik gösterebilir ve her biri ayrı ayrı başlıklar altında daha ayrıntılı ve bütünü düşünerek ele alınmalıdır.

Bu sebeple güvenliğin sağlanmasından sorumlu olan birimler, süreç sahipleri ve organizasyon yönetimlerinin iş birliği ve bilgi paylaşımı özel önem taşımaktadır.

[2] AAA (Authentication-Doğrulama, Authorization-Yetkilendirme, Accounting-İzleme)
[3] MFA (Multi Factor Authentication-Çok Faktörlü Kimlik Doğrulaması)