Process Safety Beacon
Üretim Personeli için Mesajlar
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

Bu yayının sponsoru
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

# Siber Güvenlik ve Kimyasal Operasyonlar

Temmuz 2021

*Şekil 1. Oldsmar, Florida su arıtma tesisi*

5 Şubat 2021'de Florida, Oldsmar'da bir su arıtma tesisi çalışanı, imlecin kontrol bilgisayar ekranında garip bir şekilde hareket ettiğini fark etti. Başlangıçta herhangi bir endişe yoktu. Tesis, personelin ekranları paylaşmasına ve BT sorunlarını gidermesine olanak sağlamak için uzaktan erişim yazılımı kullandı. Süpervizör, tesisin sistemlerini de izlemek için genellikle operatörün bilgisayarına bağlanırdı. Birkaç saat sonra operatör, imlecin su arıtma tesisinin kontrollerinde hareket ettiğini ve tıkladığını fark etti. Saldırgan, saniyeler içinde sistemin sodyum hidroksit ayar noktasını milyonda 100 parçadan (ppm) 11.100 ppm'ye değiştirmeye çalışıyordu. Operatör müdahaleyi çabucak fark etti ve sodyum hidroksiti normal seviyelere döndürdü. Neyse ki, su kalitesi üzerinde herhangi bir etki olmadı.

Yakın zamanda Colonial Boru hattına yapılan bir fidye yazılımı saldırısı, birkaç gün boyunca ABD'nin Doğu Kıyısı'na benzin tedarikini durdurdu.

Şirketinizin sistemleri muhtemelen internete bağlı ve siber tehditlere karşı korunma gerekiyor. Şirketler tarafından siber tehditleri caydırmak için kullanılan pek çok strateji vardır: güvenlik duvarları, anti-virüs yazılımları ve kötü amaçlı yazılımlara ve bilgisayar virüslerine karşı koruma politikaları.

Daha fazla insan uzaktan çalışıyor; bu da siber saldırı fırsatlarını artırıyor.

## Biliyor muydunuz?

- Siber suçlular, güvenlik açığından yararlanmak ve hedeflerine ulaşmak için birden fazla karmaşık kötü amaçlı yazılımlar kullanır.
- Fidye yazılımı saldırıları, organize suçluların onu para kazanma aracı olarak kullanmasıyla artıyor.
- Yakın tarihli bir araştırmaya göre, her 39 saniyede bir siber saldırı meydana geliyor. (Ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Siber tehditler, şirketin sistemlerine e-postalar, ekler aracılığıyla ve flash sürücüler veya diğer taşınabilir depolama aygıtları gibi taşınabilir depolama aygıtlarından girebilir.
- Siber güvenlik ihlallerinin yüzde doksan beşi insan hatasından kaynaklanmaktadır. (Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

## Ne yapabilirsiniz?

- Devam etmeden önce yazılım güncelleme isteklerini daima BT ile doğrulayın ve onaylanmış güncellemeleri zamanında yükleyin.
- Güvenlik duvarlarınızın ve diğer ağ yazılımlarınızın güncel ve aktif olduğundan emin olun.
- Sistemlerinizi ve verilerinizi düzenli olarak yedeklediğinizden emin olun.
- Tüm erişimler için güçlü parolalar kullanın. Şifreleri veya hesapları paylaşmayın ve şifreleri düzenli olarak değiştirin.
- Parolaları tarayıcılara kaydetmeyin.
- Tanımadığınız birinden gönderilen e-postalardaki bağlantılara veya eklere tıklamayın.
- Herhangi bir şirket bilgisayarına asla onaylanmamış yazılım yüklemeyin; erişim anahtarlarının ve diğer fiziksel güvenlik cihazlarının uygun şekilde güvenli olduğundan emin olun.
- Uzaktan erişim kullanıyorsanız, şirketin gereksinimlerine uyun. Halka açık internet sitelerini kullanıyorsanız özellikle dikkatli olun.
- Bilgisayarınızda garip veya farklı bir şey varsa, yardım isteyin! Erişim elde etmeye çalışan bir bilgisayar korsanı olabilir.

**Siber saldırılar gerçektir. Sen savunmanın hayati bir parçasısın.**