4. ENDÜSTRİ DEVRİMİ VE BİLGİ GÜVENLİĞİ

Farklı evrelerde süregelen Endüstri Devrimi dünyada birçok yenilik hareketinin, modernliğin ve dönüşümün temeli olarak görülüyor. Endüstri Devrimi süreci başlamadan önce ekonomik yapı büyük oranda tarım ve hayvancılığa bağlıydı ve dokumacılık, marangozluk, demircilik gibi tarım dışı üretim de esnaf ve zanaatkârlar tarafından, elle çalıştırılan tezgâhlarda gerçekleşiyordu. Buhar makinesinin icadı ile tetiklenen Endüstri Devrimi, toprağa, tarıma ve insan gücüne dayalı ekonomiden, makineleşme ve seri üretimle şekillenen yeni ve farklı bir ekonomik yapıya geçişi sağladı.

Endüstrileşmenin ikinci aşaması temel hammadde ve enerji kaynaklarındaki değişikliklerle ortaya çıktı. Buhar, kömür ve demirin yanı sıra çelik, elektrik, petrol ve kimyasal maddelerde üretim sürecinde kullanılmaya başlandı.

1970'lerden bugüne kadar süren döneme Üçüncü Endüstri Devrimi hâkim oldu. İkinci Dünya Savaşı sonrasında, elektronik, bilgi ve iletişim teknolojilerinin gelişimiyle birlikte üretimin otomasyonu sağlandı.

Günümüzde, üretime yönelik dijital teknolojiler arasında yeni nesil otomasyon sistemleri ve nesnelerin interneti kavramı yer alıyor. Endüstri 4.0, ortaya çıkışıyla beraber üretimi durdurabilecek büyük bir riski de beraberinde getiriyor: **Siber saldırılar!**

Siber saldırı yaşamayacağız diye bir kavram geride kaldı. Siber saldırı yaşayacağız. Bizlerin artık zararı nasıl azaltacağız sorularının cevabını veriyor olmamız lazım.

İş ortaklarının, tedarikçilerin güvenlik süreçlerine entegre edilmesi ve en zayıf halkanın (çalışan/insan) eğitilmesi de Endüstri 4.0 devriminde güvenliği sağlamak için önemli maddelerden biridir.

Bilgilerin sadece bilmesi gereken prensibi doğrultusunda erişim yetkisi olan kişide olması ve başkalarının görmemesi kapsamında bilgi güvenliğinin üç unsuru, ***gizlilik, bütünlük ve kullanılabilirlik*** Endüstri 4.0 siber güvenliği açısından hayati önem taşımaktadır.

İnsanın, geçmişten bugüne, gıda ve barınma ihtiyacından sonraki en temel dürtüsünün güvenlik üzerine olduğu hepimizin bildiği bir konudur. Güvenlik tedbirlerindeki gelişmeler de, periyodik olarak yaşanan olaylara paralel gelişim gösteriyor. Hangi alanda bir güvenlik eksiği oluşursa o alanda sistemler gelişiyor veya mevcut ürünler o alanda daha çok kullanılmaya başlanıyor.

Güvenlik hususu düşünülmeden devreye alınmış sistemlerin aniden savunmasız kalışına tanık olabiliriz. Dördüncü Sanayi Devrimi'nde hayatımızın her alanında birbiri ile konuşan ve haberleşen cihaz, sistem ve robotlar olacakken güvenlikten bahsetmemek olmaz. Peki, bu kadar teknolojik ürün ve sistem yüzde yüz güvenlik içinde çalışabilir mi? Keşke cevabı "evet" olabilse idi. Önce, bir fabrika hayal edelim; fabrikaya gelen hammaddeler insansız araçlarla geliyor, otomatik olarak robotlarla indiriliyor ve hammadde robotik tezgâhlarda işlenmeye başlanıyor. Üretilecek mamulün ebadı, cinsi, rengi ve diğer tüm özellikleri programlanıyor ve ürün satışa hazır hale geliyor. İşte bu süreç içinde minimum insan gücü ve maksimum robot ve bilgisayar gücü olacak. Bu bilgisayar ve robotlar yapay bir zekâ ile birbiri ile konuşacak ve üretimin her anında belirlenen kurallar ve kodlar çerçevesinde üretim yapacak. Peki, bu kuralları ve kodları değiştirmeye, bozmaya ve işlemez hale getirmeye çalışan olursa ne olacak? Sonuçta her şey kablolu ya da kablosuz olarak bir ağa bağlı ve bu ağda bir kimlik olarak yer almaktadır. İşte bu ağa sızan kötü niyetli birisi o fabrikayı savaş alanına çevirebilir ve telafisi mümkün olmayan hasarlara neden olabilir.

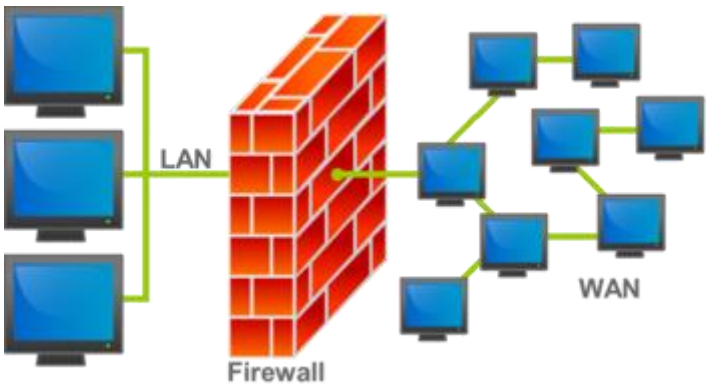
Yüksek profilli siber saldırıların sıklığı ve karmaşıklığı, siber suçların gerçek ve ciddi bir risk olduğuna işaret ediyor. Şirketler ve devlet kurumları, ağlarını dış saldırılardan korumak için sıkı güvenlik önlemleri uyguluyor olsalar da, çoğu güvenlik riskinin korkutucu bir bölümünün içeriden olduğunu bilmiyorlar.

Siber güvenlik farkındalığı tüm çalışanlara yayılmalıdır. İşten ayrılan bir personel, şirketten alacağı bilgi ya da yazılım ile saldırı gerçekleştirebilir. Ağa eklenen her bir cihaz, siber saldırılar için ağa olası bir giriş noktası sağladığından, potansiyel bir zayıf nokta veya zafiyet yaratır.

Yukarıda bahsedilen konuların dışında bilgi güvenliğini sağlamada kullanılabilecek teknolojik uygulamaların bazılarından bahsedecek olursak;

Firewall (Güvenlik Duvarı)

İnternet gibi açık (public) bilgisayar ağlarına erişim (bilgi alışverişi), kullanıcılara ve şirketlere ait verilerin güvenliğini sürekli tehdit etmektedir. Ziyaret edilen bir site, alınan bir e-posta ya da indirilen bir dosyada bulunan zararlı bir içerik bilgisayarlara zarar verebilir hatta bilgilerin çalınmasına neden olabilir. Bunun dışında uzaktan erişim gereksiniminin (VPN bağlantısı) artması şirket ağlarını ve bilgisayarlarını tehlikeye sokmaktadır. İşte *firewall*'lar şirket ağlarındaki verilerin dış ağlar, internet ya da uzak bağlantılardan gelen risklere karşı korunmasını sağlar.



Kriptografi (Şifreleme Teknolojileri)

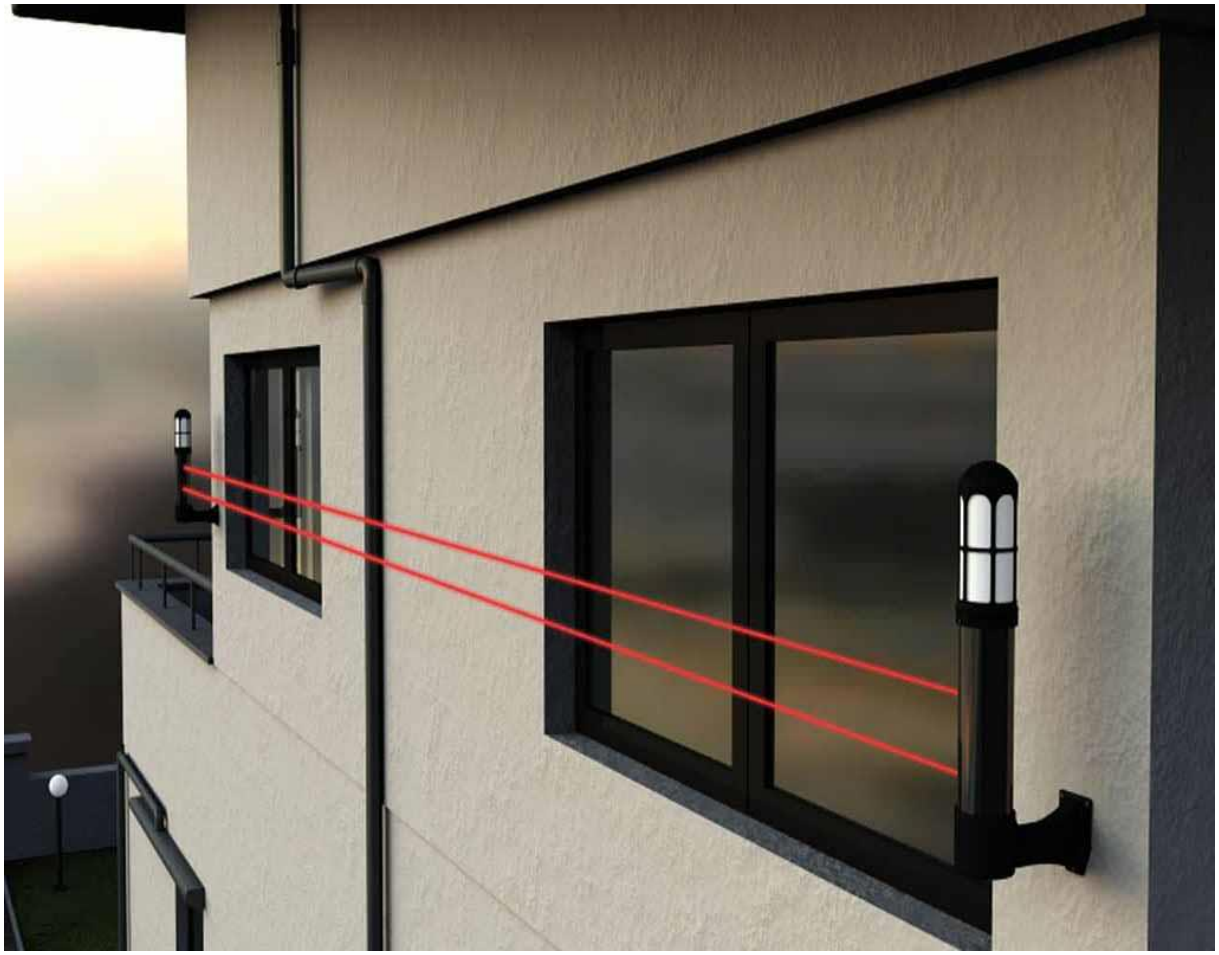
Bilgi güvenliğinin en önemli prensiplerinden biri hiç şüphesiz bilgilerin gizliliğini (*confidentiality*) ve bütünlüğünü (*integrity*) sağlamaktır. Bu kavramı desteklemek için ayrıca bilgilerin izinsiz olarak değiştirilmesini de engellemek gerekir. İşte "kriptografi", verilerin gizliliğinin ve bütünlüğünün sağlanması alanında çalışan bir bilim dalıdır. Günümüz bilgi teknoloji uygulamalarında kriptografi, verilerin şifrelenmesi, bilgisayar parolalarının gizlenmesi, e-ticaret ve dijital imza gibi konularda çok önemli bir yere sahiptir.

Zayıflık Analizi (Vulnerability Analysis)

Bilgi güvenliğinin amacı bilgisayarlarımızı ve bilgisayar ağımızı içeriden ve dışarıdan gelebilecek saldırılara karşı korumaktır. Bunu yapmadan önce mantıklı olarak kendi açıklarımızı (zayıflıklarımızı ve zafiyetlerimizi) görmek isteriz ve buna göre önlem alırız. İşte bu temelde "zayıflık analizi" çalışması yapılır.

Fiziksel ve Çevresel Güvenlik

Fiziksel güvenlik, bilgi güvenliğinde özellikle bilgisayar sistemleri, sistem odası, önemli alanlar ve odaların yetkisiz girişlere ve doğal afetlere karşı korunmasını sağlamaktır. İlk güvenlik aşaması olarak değerlendirilen fiziksel güvenlik, bilgisayar/sistem odalarına girişi, sistemlere zarar verebilecek tehlikelere karşı önlemleri kapsar. Fiziksel ve çevresel güvenlik önlemleri başta doğal afetler olmak üzere çok sayıda tehdide karşı önlemlerin alınmasını sağlamalıdır.



Sonuç olarak hem üretim hem de ortaya çıkarılabilecek yeni ürünlerin geliştirilmesi aşamasında siber güvenlik, Endüstri 4.0 alanında mutlaka ön planda tutulmalıdır. Sanayide Endüstri 4.0 genelinde kullanılacak cihazların ve kurulacak olan sistemlerin mutlaka güvenlik testlerinin yapılması gerekmektedir. Ülkelerin, endüstri alanında elde ettikleri bilgi ve becerilerin başka ülkeler tarafından çalınmaması ve bilgi hırsızlığına maruz kalmamak için, siber güvenlik alanındaki çalışmaları ön plana almaları gerekmektedir.

Oğuz TAŞBOLAT

KalDer Üyesi

TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.

Kalite Yönetim Sistemleri Sorumlusu