KRİTİK ALTYAPILAR VE SİBER GÜVENLİK

Gökay TÜRKSÖNMEZ - EMO Ankara Şubesi Kritik Altyapılar ve Siber Güvenlik Komisyonu Başkanı
Elektronik Mühendisi
gokaytr@gmail.com

GİRİŞ

Ekonomik Kalkınma ve İşbirliği Örgütü (OECD); kritik altyapıları; fonksiyonelliğini yitirmesi durumunda sağlık hizmetlerine, toplumsal emniyet ve güvenliğe, ekonomik büyümeye veya ekonominin verimli çalışmasına ciddi yönde etki eden bilgi ağları ve sistemleri olarak tanımlamaktadır (OECD, 2022).

Bu kapsamda aşağıda sıralanan maddelerde ülkelerin genel olarak kabul ettikleri kritik altyapılar gösterilmektedir.

- Elektronik Haberleşme
- Enerji
- Bankacılık ve Finans
- Kritik Kamu Hizmetleri
- Ulaştırma
- Su Yönetimi altyapılarıdır.

Bilgi teknolojileri istisnasız olarak bütün kritik altyapılarda kullanmaktadır. Elektronik Haberleşme (İletişim altyapısı, Internet altyapısı) gibi kritik altyapılar ise tamamen bilgi teknolojileri bileşenlerinden oluşmaktadırlar.

Enerji üretim tesisleri, barajlar, fabrikalar gibi kritik altyapılar SCADA olarak adlandırılan ve bu yapıları kontrol eden ve izleyen bilgi teknolojilerini içermektedirler.

Endüstri 4.0 sürecini geçtiğimiz andan itibaren; daha önce kendi içerisinde Otomasyon Teknolojileri (OT) ile kapalı çalışan Kritik Altyapı kuruluşları; üretimde verimliliğin artırılması, dijital dönüşüm süreçleri ile özellikle lojistik kapsamındaki hizmetlerin üretim sürecine entegre edilmesi, ayrıca enerji verimliliği ve tek merkezden yönetim kolaylığı gibi sebeplerden dolayı internet altyapısını yoğunlukla kullanmaya başlamışlardır. Bu bağlamda, saldırı yüzeyinin artmış olması OT altyapısını kullanan bütün kuruluşları, siber güvenlik önlemlerini de dikkate alarak gerekli tedbirleri almaya zorunlu kılmaktadır.

Bu yazımızda özellikle Otomasyon (OT) Altyapılarına yapılacak saldırılardan bahsedeceğim.

Her alanda yapılan siber saldırılara karşı koyabilmek için; kuruluşların ilgili ekiplerinin mücadele etmesi, yorucu zamanlar geçirmesi ve olağan ya da olağandışı maliyetlere hazırlanması gerekmekte. Ancak OT altyapılarında saldırılara karşı koymak daha özel uğraşlar gerektirebilir. Gerçek zamanlı çalışan fiziki sistemlerin devamlılığı ve insan hayatının güvenliği için biraz daha kaygılanmamız gerekecektir.

SİBER OLAYLAR HERKESİN BAŞINA GELEBİLİR

Saha tecrübelerimiz şunu gösterdi ki; herhangi bir siber saldırıya maruz kalan teknik ekiplerin en genel kanıları: "Bizim başımıza geleceğini düşünmemiştik" yaklaşımı olmakta. Bunun altında bazı psikolojik etkilerin olduğu muhakkak. Kendisini bir saldırı hedefi olarak düşünmemek, herhangi bir siber olay yaşamayacağı düşüncesi ile hazırlıklı olduğuna yönelik eksik/yanlış kanı ya da riski gerçekten göz ardı etmek.

Amerikan Ulusal Standartlar ve Teknoloji Enstütüsü'nün (NIST) Siber Tehdit tanımını paylaşmak isterim. "Siber tehdit' terimi, internet üzerinde faaliyet gösteren kötü niyetli kişiler veya gruplar tarafından gerçekleştirilen, sıradan insanlardan devletlere kadar risk oluşturulabilecek zarar verici eylemleri ifade eder. Siber tehditler; bilgisayar sistemleri, ağlar, tesisler, internet kullanıcıları ve dijital varlıklar üzerinde olumsuz etkilere neden olabilir."

NIST'in bu tanımından hareketle; herhangi bir sis-

teminiz internet ya da herhangi bir ağa bağlıysa, kuruluşunuzun ne kadar küçük ya da büyük olduğuna bakılmaksızın TEHLİKE ALTINDASINIZ demektir. Bundan kurtulmanın yolu ise sistemlerinizi 19ncu yüzyıl standartlarına geri göndermek değil (ağdan ayırmak), gerekli ve yeterli tedbirleri almaktır.

Kuruluşlar, büyük bir siber güvenlik olayı yaşayamayacak kadar büyük ve hazırlıklı (!) olduklarından, ya da hedef olamayacak kadar küçük olduklarından ya da ilgi çekici olmadıklarından kendilerinden gayet emin yaşıyorlar. Bu konforlu yaklaşım sayesindedir ki, siber güvenlik olayları herhangi bir sektördeki, her şekil ve büyüklükteki organizasyonun başına gelebiliyor. Büyük kuruluşlar, riskleri azaltma hızı ve tehdit yüzeylerinin belirlenmesinin yanı sıra tam mimari üzerinde birbirini tetikleyen risklere karşı farkındalık konusunda da zorluklarla karşı karşıya kalıyorlar. En iyi savunulan kuruluşlar bile sıfırıncı gün (zero-day) saldırıları, aralıklı gözetimler veya sabırlı/kararlı düşmanlar/rakipler nedeniyle mağdur edilebiliyor.

Küçük kuruluşlar, eksik altyapıları yüzünden, iş ortaklarına veya müşterilere yönelik saldırı vektörleri olarak veya gelecekteki endüstriyel saldırılar için test ortamları olarak kullanılabiliyor. Yani paydaşlar serisi ile hazırlanan bir iş sürecinde maalesef EN ZAYIF HALKA olmaktalar.

OT Altyapıları için; her şeyden önce fiziksel sonuçları ve süreçleri düşünmek, insan hayatı, tesis, insan ve çevre güvenliği ve süreçlerin doğru işlemesi sonuçlarıyla ilgilenmek zorundayız. Ve en ufak bir ihmalin doğuracağı sonuçların analizi yapılırken siber güvenlik tehditlerinin de en ön sıralarda değerlendirilmesi gerekir. İyileştirme çabaları sırasında geçmişte yaşanmış olaylardan (kuruluş içinde yaşanmış ya da kamuya açık olaylar), gözlemlerden dersler çıkarılabilir, devam eden süreçlere (programlar, projeler) ve personele destek verilebilir. Mevcut farkındalığın geliştirilmesiyle, siber suçluların kurbanı olduğunuzu/olabileceğinizi ve yalnızca gelişmiş güvenlik önlemleriyle bu saldırganlarla savaşabileceğinizi unutmayın.

OT ALTYAPILARI ÖZELİNDE PLANLAMA YAPMAK

Bir siber güvenlik olayının herhangi bir kuruluşun başına gelebileceğini, bu olaylarla başa çıkmak için test edilmiş ve yaygınlaştırılmış etkili bir plana sahip olmanın, o kıyamet gününde hayatta kalmanın ayrılmaz bir parçası olduğunu akıldan çıkarmamalıyız.

Kuruluşlar tarafından genel bir Kurumsal Bilgi Sistemi (KBS/BT) Olay Müdahale planına sahip olmak çok önemlidir, ancak bu plan operasyonel ortamlara hizmet etmek için yeterli değildir. OT olay müdahalesine yönelik planlama, çeşitli yönlerden BT olay müdahalesinden büyük ölçüde farklıdır; her şeyden önce, bu olayların gerçek ve fiziksel sonuçları olacaktır ve bunlara verilecek karşılıklar da farklı olmalıdır.

Bu kapsamda istinasız tüm kuruluşlar için, mümkün olan en kısa sürede yönetim desteğiyle yürütme yetkisine sahip bir planı uygulamaya koymaya yüksek öncelik verilmelidir. Oldukça olgun bir BT olay müdahale planına sahip kuruluşlar için bile, ayrı bir tamamlayıcı OT müdahale planı geliştirmeleri veya merkezi plan boyunca OT için net eklentileri belirlemeleri gerekir. Bütün bu çalışmalar yapılırken süreç ve güvenlik sonuçlarının da düşünülmesi; Siber güvenlik Planının yaşam döngüsü aşamalarının her bir adımında, OT'deki kendine özel süreçler dikkate alınarak risk matrisleri oluşturulmalı, önem derecesi ve iletişim planları gibi bölümler ayrı olarak hazırlanmalı ve OT personeli de bu talimatların oluşturulması ve test edilmesinde sürece dahil edilmelidir. Çünkü, OT'de süreçleri kontrol altına almak çoğu zaman BT ortamlarına göre çok daha farklı olacaktır. Bu yalnızca Adli Bilişim (Forensics) ve kurtarma üzerinde değil, aynı zamanda süreçlerin yeniden kararlı haline döndürülmesi üzerinde de önemli farklılıklar olarak gözlemlenecektir. Bu nedenle, süreç ortamlarını kontrol altına alma yetkisi muhtemelen siber güvenlik ekibine ait olmayacaktır.

Ek olarak, eski ve düşük seviyeli sistemlerin, potansiyel süreç etkisi, modern güvenlik araçlarının eksikliği, hatta endüstriyel cihazların fiziksel erişilebilirliği nedeniyle adli bilişim incelemeleri ve kök neden analizi de oldukça farklı olacaktır. Adli bilişim incelemeleri ve kök neden analizinin ayrıntılı olarak gerçekleştirilmesinin fizibilitesi bile, acil yaşam ve güvenlik endişeleri nedeniyle farklılık gösterebilir. İletişim bile (özellikle çalışma saatleri dışında) süreç ortamında benzersiz zorluklar yaratan bir alandır.

KÜÇÜK DOKUNUŞLAR, BÜYÜK ETKİ

OT ortamlarında karşılaşılan daha organize ve karmaşık saldırılar da mevcut. İş süreçlerine etki yeteneklerini geliştiren devlet kaynaklı saldırıların ardı arkası kesilmiyor. Ulusal/uluslararası medyada gözlemlenen haberlerde gördüğümüz kadarıyla; karşılıklı hasmane duygularla birbirlerine saldıran Rusya-Ukrayna, İran-İsrail, İran-Amerika, Çin-Amerika, Kuzey Kore-.....

Bu haberlerde devlet destekli saldırıların siber dünyayı nasıl bir savaş alanına döndürdüklerini ve kritik altyapıların (Elektrik, Su Altyapıları, Telekomünikasyon, Endüstriyel Üretim vb.) saldırganların kontrolüne geçmesiyle sivil insanların bundan nasıl olumsuz etkileneceklerini kaygıyla izleyebiliyoruz.

OT altyapılarının güvenliğini sağlamak, birçok insani ve teknolojik nedenden (insani zafiyetler ve eksik teknolojik olgunluk) dolayı zordur. Saldırganlar tarafından, sistemlerin ele geçirilmesinde ve etki alanının genişlemesinde rolü olan izinsiz girişlerin büyük bir kısmı hala nispeten çok basit yollarla başlatılıyor. OT ağları güvenlik mimarisi ve teknolojisi açısından hâlâ biraz geride kalıyor. Bu, altyapılarda kullanılan sistemler için daha uzun yaşam döngülerinden, bir kısmının yeterli olgunluk düzeyinde tasarlanmamış olmasından ve bir kısmının da sadece zorunlu olarak kullanılmasından kaynaklanmaktadır. Operasyonel süreçler basitçe çalışmalıdır ve konu şifreleme ve güvenlik araçlarına geldiğinde fazla karmaşık hale gelmemelidir.

Halbuki birçok siber olay, 5 aşamalı temel bir OT Siber Güvenlik Kritik Kontrolü aracılığıyla hâlâ önlenebilir. Olay müdahale planlamasının hazırlanmasına ek olarak, güvenli ağ mimarisinin, ağ görünürlüğünün ve sürekli izlemenin, uzaktan erişim kontrolünün ve güvenlik açığı yönetiminin hafifletici önlemler olarak ne kadar önemli olduğunun bilinmesi gerekir. Bunlar, deneyimli siber güvenlik uzmanları için kâğıt üzerinde basit görünebilir, ancak bunlar genellikle gözden kaçırılır, yeterli kaynak sağlanmaz veya OT ortamlarında göz ardı edilir. Ayrıca uygulanması daha zorlayıcı ve ince mühendislik gerektirebilir.

Tüm bu tedbirlerin ışığında gözle görülmeyen bir koruma kalkanı tesis edilebilir. Dünyada, OT alanında karşılaşılan siber suç gruplarının büyük bir çoğunluğunun rakip işletmeler olduğu istatistiksel olarak kanıtlanmıştır. Maalesef bazı kuruluşlar, etik olmayan bir şekilde, mümkün olan en fazla kazancı elde etmek için en az direnç gösterilen yolu seçiyor, rakiplerine bel altı saldırıyorlar. Bu kapsamda; siber güvenlik altyapılarını kurmuş kuruluşlar onlara gayelerine ulaşamayacakları bir set kurmuş olacaklar. Her saldırı girişimlerinde, tekrarlanan engellere çarpacakları bir rakip kesinlikle onların başarısız olmasına veya pes etmesine neden olabilir.

Tüm bunlar kulağa ürkütücü gelebilir. Ancak endüstriyel ortamlarınızda temel güvenlik kontrolleri konusunda yapacağınız her küçük adım büyük bir fark yaratabilir! Yönetilebilir değişikliklerle uğraşarak ve karmaşık olanları projelendirmek için uzmanların desteğini alarak işe başlamalısınız.

MEVCUT DURUMUN ANALİZİ VE GELİŞTİRİLMESİ

OT siber güvenlik olgunluğunuzu geliştirmeye başladıktan sonra, planlarınızı ve güvenlik önlemlerinizi düzenli olarak test etmeniz ve mevcut durumunuzla, büyüyebileceğiniz alan konusunda gerçek, önyargısız ve tarafsız bir görünüm elde etmeniz gerekir.

OT'de mevcut durum analizi değerlendirmeleri genelde zordur. Ancak bu değerlendirmeler, bir ortamın teknik siber güvenlik durumu (ve aslında yapının kendisi) hakkında bir anlayış oluşturmak için çok yararlı bir araç olabilirler (özellikle kurumsal siber güvenlik araçlarından ve programlarından izole edilmişse).

Herhangi bir kırmızı takım değerlendirmesi veya sızma testinden önce, ilk başta pasif mimari değerlendirmelerin yapılması istenir. Tüm değerlendirmeler, OT siber güvenliği konusunda uygun şekilde eğitilmiş personel tarafından, OT liderlerinin onayı ile belirlenmiş uygun düşük etkili süreçler ortamında gerçekleştirilmelidir.

Son olarak, olaya müdahale planları ve prosedürler için rutin masa üstü tatbikatları ve taktiksel tatbikatlar da planlanmalıdır. OT personeli ve Yönetimin de dahil olması ile çeşitli paydaşların katılımı sağlanmalıdır. Planların gerçekten işe yarayıp yaramadığının güvenli bir alanda keşfedileceği yer burasıdır. Bir kriz sırasında değil, bir tatbikat sırasında kazanılan dersleri öğrenmek çok daha kolaydır. Sağlıklı bir "hata yok" tutumuyla yapılan çalışmalar aynı zamanda BT ve OT personeli arasında mükemmel bir ilişki kurulmasını da sağlar.

BT ve OT EKİPLERİNİN İLİŞKİLERİNİN GELİŞTİRİLMESİ

Pek çok kuruluşta, siber güvenlik ile OT personeli arasındaki ilişkiler son derece gergin bir ortamda gelişir. Yıllarca süren yanlış ve yetersiz iletişim; OT'yi bir BT kutusuna sığdırmaya yönelik beceriksiz çabalar nedeniyle zarar görmektedir. Bu ilişkiyi onarmak ve ekipler arasında sağlıklı iş birliği ve iletişim hatları kurmaya yönelik kararlı bir çabanın üretilmesi çok önemli. Bu ilişki kurulamadığı anda, bir kriz anında grupların arasındaki siyaset ve hamaset, müdahale çabalarını engelleyebilir. Bilmeden saldırganlara yardım edebilirler.

Güveni yeniden inşa etmek zordur. BT personeli, süreç sistemleri hakkında hiçbir zaman mühendisler ve operatörler kadar bilgi sahibi olamayacaklarını; operatörler ve mühendisler de sürecin güvenli ve güvenilir bir şekilde ilerlemesine yardımcı olmak için masaya getirilen siber güvenlik bilgisine ve çözümlerine saygı duymaları gerektiğini kabullenecek bir yaklaşım sergilemelidir. Üst Yönetimler tarafından onaylanmış iş gözetimi programları, OT personelinin olay müdahalesinde etkin olarak görevlendirilmesine olanak tanıyan çalışmalar ve uygulamalar ile bu sürecin de kendine has bir otomasyona çevrilmesi sağlanabilir. Sonuçta en önemli şey, iki ekibin saygıyı paylaşması ve ortak bir misyona sahip olması: personeli hayatta ve güvende tutmak ve fiziksel süreçlerinin sorunsuz işlemesi.

OT RİSK TRENDİ VE YÖNETİMİ

OT Siber güvenlik riskleri yıldan yıla artmaya devam ediyor. Yıllara sair yapılan anketler ve incelemelere göre; Son 5 yıla baktığımızda 2019'da ankete yanıt verenlerin %38'i OT altyapılarına yönelik tehditleri "yüksek kritik" olarak değerlendirmişti. Bu oranın 2021'de %40'a, 2022'de %41'e ve 2023'te %44'e yükseldiğini gözlemlemekteyiz. (Veriler SANS ICS Annually Report yayınlarından derlenmiştir)

Bu değerlendirme, fidye yazılımı saldırılarıyla kritik altyapılara yönelik artan ve CRASHOVERRIDE ve PIPEDREAM gibi ölçeklenebilir OT hedefli saldırı çerçevelerinden etkilenen kuruluşların açık edilmesinden sonra yapılan çalışmaların sonuçlarıdır. Bu kamuoyu bildirimlerinin, sektörel farkındalık yönünden olumlu etkileri olmakla beraber, daha fazla OT saldırı aktörünün, daha az kötü amaçlı yazılım kullanarak etki yaratmasına olanak tanıyacak cesareti bulmasına da olanak tanımaktadır. İçsel kanıları: "Bu kadar kolay mı?" olacak, motivasyonları artacaktır.

OT TEKNOLOJİ TRENDİ

İyi tasarlanmış, kapsamlı bir OT savunma güvenlik programına sahip olmak bir lüks/opsiyon değil, esas olmalıdır. O durumda dahi, kritik altyapı tesislerinin, kritik altyapıyı proaktif bir şekilde savunmak için temel pasif ve önleyici kontrollerin ötesine geçmesi gerekir. Mühendislik ve güvenliğe öncelik verirken modern tehditleri tespit etmek ve bunlara karşı savunma yapmak için de olgun OT Güvenlik altyapıları kurulmalıdır.

Bunun için;

- BT ve OT arasındaki yapısal farklılıkların benimsenmesi
- OT uyumlu kontrollerin belirlenmesi,
- Proaktif OT tehdit avcılığı için eğitimli personelin ve özel araçların kullanımının planlanması,
- OT-Özel güvenlik bütçelerinin planlanması,
- OT'ye özgü ağ görünürlük çözümlerinin yaygınlaştırılması en temelde yapılması gereken işlemlerdir.

2023 YILININ ŞAŞIRTICI BULGULARI: TAKTİK VE STRATEJİK SAVUNMA HAMLELERİ

2023 anket verilerinden elde edilen endişe verici beş çıkarım.

1'İNCİ BULGU

Tüm dünyadaki (Türkiye'de bu oran çok daha düşük) OT tesislerinin yalnızca %52'sinde belgelenen, masa üstü çalışmalarıyla test edilen ve güncel tutulan OT'ye özgü bir olay müdahale planı bulunmaktadır. %17'si böyle özel bir OT olay müdahale planına sahip olup olmadığından emin değil. Bunun nedeni, aynı kuruluşların güncel ve test edilmiş bir BT olay müdahale planının da olmamasıdır. BT güvenlik kontrollerini bir OT tesisinin olay müdahale planına "kopyalayıp yapıştırmak" işe yaramayacaktır. Kendisinde bu planın olduğunu iddia edenler içinde bu yaklaşıma sahip olanların da olduğunu bildirmeliyiz. Ancak bu yaklaşımın güvenlik ve mühendislik operasyonlarında ciddi, istenmeyen veya felaketle sonuçlanabilecek sonuçlara yol açması muhtemeldir.

Stratejik Hareket

Tesisler/Kuruluşlar, OT'ye özel mühendislik odaklı bir olay müdahale planına sahip olarak en iyi uygulamaları karşılayacak şekilde tasarlanmalıdır. Masa başı tatbikat planları sektöre özel tehdit istihbaratından elde edilen gerçekçi senaryolarla

beslenerek bu planlar düzenli olarak uygulanmalıdır. Tatbikatlarda iş birliği ve farkındalığın artması maksadıyla ilgili tüm ekiplerin dahil edilmesi ve mühendislik ekibinin sorumluluğu üstlenmesi sağlanmalıdır. Bu şekilde mühendislik personeliyle saygın ilişkiler kurulması, BT ve OT ekipleri arasındaki boşlukların kapatılması ve güvenlik ve kontrol sistemlerine öncelik verilmesi tetiklenebilir.

Taktiksel Hareket

OT siber güvenlik uzmanları, BT güvenlik becerilerinden yararlanmalı ve BT ile OT'nin farklı olduğu alanlarda genel siber güvenlik planlarına destek olmalıdır. Bunun ötesinde, güvenliğe öncelik verirken, OT'ye özgü kontrolleri, teknolojileri ve süreçleri kullanarak OT'ye özgü tehditlere aktif olarak yanıt vermek için BT güvenliğinden nelerin uyarlanabileceğini keşfetmeleri gerekecektir. Mühendislik sistemlerinin ağ düzeyinde nasıl çalıştığını ve mevcut olmayan veya rakipler tarafından manipüle edilen öncelikli OT/EKS (Endüstriyel Kontrol Sistemleri) cihazları/kontrolörleri/uzak terminal birimlerine ne tür saldırılar yapılabileceği öğrenilmelidir. Bunun için OT-Özel MITRE ATTACK vektörlerinden faydalanılması gerekecektir.

2'NCİ BULGU

2023 yılında çoğu tesis, OT ağlarının, BT ağları ve İnternet gibi bazılarının düşman ağlar olarak adlandırdığı, nispeten koruması olmayan ağlardan iyi bir şekilde ayrıldığını ve korunduğunu büyük bir güvenle belirtiyor. Ancak %38'i, EKS/OT'ye yönelik ihlallerin ilk saldırı vektörünün, tehditlerin EKS ağına girmesine izin veren BT ağlarından geldiğini bilmiyor.

Stratejik Hareket

Öncelikle ağ mimarisine odaklanılmalı, ekipler ve bütçe en yüksek yatırım getirisi (Otomasyon süreçlerinin aksamasıyla yaşanacak kaybın daha fazla olacağı değerlendirmesiyle) sağlayacak şekilde planlanmalıdır. Güçlü bir ağ mimarisi ve korunaksız ağlardan sıkı bir şekilde izole edilmiş bölümlendirme üzerine inşa edilen tüm savunma kontrolleri ve süreçleri, çok daha yüksek bir yatırım getirisine sahip olacak ve en önemli olanı koruyacaktır. Diğer ilave faydalar, endüstriyel olaylara müdahale koşulları sırasında kontrol altına almaya yöneliktir.

Taktiksel Hareket

BT, EKS/OT ve İnternet arasındaki tüm güvenilir bilinen (ve bilinmeyen) erişim kuralları incelenmeli, OT ağına erişimde kullanılan güvenlik duvarı erişim kontrol listeleri gözden geçirilmeli ve EKS'ye giren ve çıkan bağlantılara uzaktan erişim yoluyla gerçekleştirilebilecek saldırılara karşı ek tedbirler alınmalıdır.

3'ÜNCÜ BULGU

Penetrasyon testlerinin %47'si Purdue Modelindeki Seviye 2 cihazlara yöneliktir. Bu durum endişe verici olabilmektedir. Çünkü mühendisliğe özgü cihazlarda yanlış şekilde gerçekleştirilen EKS sızma testi; güvenliği, güvenilirliği ve operasyonları doğrudan olumsuz yönde etkileyebilir.

Peki EKS/OT ortamlarında penetrasyon testi yapabilir misiniz?

Evet. Ancak herhangi bir seviyedeki EKS sızma testi ile güvenliğin sürdürülmesi isteniyorsa, OT ortamında gerçekleştirilecek en kritik süreçlerin yakınında olmamalıdır.

Stratejik Hareket

İlk önce en temel kontrollerle başlanmalıdır. Beş Kritik Siber Güvenlik Kontrolünün tümü eksiksiz bir şekilde tamamlanmalıdır. Buradan çıkarılacak Olgunluk Değerlendirmesine göre, bir üst seviyeye uygun çalışmalar başlayabilir. Otomasyon sahası Mühendislik ekiplerinin bu alandaki kararları vermesinin güvenlik açısından en iyisi olduğu bilinerek model işletilmelidir. Yeterince olgunlaştığında tesisler güvenlik ve mühendislik operasyonlarına gönül rahatlığıyla dönebilirler.

Taktiksel Hareket

Gerçek dünyadaki saldırı senaryoları üzerinden testler uygulanmalıdır. İşletme tarafından onaylandığında, ilk erişimi ve BT genelinde yanal hareketin ilgili tespit yeteneklerini test etmek için sızma testine başlanır. Sonra aşama aşama her seviye için uygun güvenlik kontrolleri test edilmeye başlanır. Testler üretim sistemlerindeki bileşenlere geldiğinde dikkatli olunmalı ve mühendisliği etkileyebilecek herhangi bir sistem üzerinde test yapılıyorsa, sistemlerin BT ve/veya OT ağlarında olup olmadığına bakılmaksızın ekstra özen gösterilmelidir. Bu tür testleri yapmadan önce daima ön onay alınmalı ve masa başı çalışmalarıyla operasyon riski en aza indirilmelidir.

4'ÜNCÜ BULGU

OT tesislerinin yalnızca %22'si, modern OT'ye özgü tehdit algılama yeteneklerini anlamak için MITRE ATTACK vektörünü kullanıyor. Bu çerçevenin etkin kullanılması, proaktif bir OT siber güvenlik programını yönlendirebilir.

Stratejik Hareket

Tesislerin siber güvenlik bilincinin artırılması ile çok daha fazla tesis, geri planda kalmak ve yalnızca reaktif olmak yerine, proaktif savunma için MITRE ATTACK çerçevesinden yararlanabilir. Aktif düşman yeteneklerini anlamak için sektördeki tehdit istihbaratından yararlanılmalıdır. Siber güvenlik ekipleri, önemli EKS veri kaynaklarını, ilgili araçları ve risk

azaltma tekniklerini belirlemek gibi proaktif görevlere hazırlanmak için teknik araçlardan ve teknik analizden yararlanma konusunda güçlendirilmelidir.

Taktiksel Hareket

OT için MITRE ATTACK kılavuzunun nasıl kullanacağı öğrenilmelidir. Saldırganlar tarafında etkin olarak kullanılan Teknik, Taktik ve Prosedürler (TTPs) incelenmeli ve kuruluşlar kendilerine göre tehdit haritası çıkarmalıdırlar. OT-SIEM kuralları için kullanılacak veri kaynakları ve OT tehdit avcılığının başlatılacağı alanlar belirlenmelidir.

5'İNCİ BULGU

Katılımcılar, OT'ye özgü ağ görünürlüğünü (NDR çözümleri), EKS ağlarında konuşlandırılması gereken ve EKS eğitimli uzmanların günlük olarak kullanması gereken en önemli yetenekler arasında birinci sıraya koymaktalar.

OT'ye özel ağ görünürlüğünün uygun şekilde tasarlanması, varlıklar ve güvenlik açığı bilgileri hakkında ayrıntıları ve güncel saldırılar da dahil olmak üzere saldırı hazırlık tekniklerini gözlemlemek için kapsamlı bir veri kaynağı sağlar. Ek olarak, endüstriyel olaylara müdahale çalışmaları ve daha fazlası için ağ trafiği verileri sağlam kaynaklar olarak değerlendirilebilir. Bu alandaki en yaygın çözümler, bu verileri, daha az güvenli olan aktif tarama seçeneği yerine, aktif sorgulamayı gerçekleştirmek için ağ trafiğini pasif olarak gözlemleyen ve bilinen tehlikeler doğrultusunda alarmlar üreterek ilgili ekipleri yönlendiren IDS (Intrusion Detection Systems) çözümleridir. Ancak böyle bir çözümün endüstriyel ağlara yerleştirilmesi kritik öneme sahiptir. Çözümün projelendirilmesi ve uygulanması (düşük maliyetli veya ücretsiz ya da profesyonel araçlar) tamamlandıktan sonra, özellikle BT ve OT güvenliği konusunda eğitilmiş personelin takibi için rehberlerin hazırlanması gerekir.

Stratejik Hareket

Üst yönetimler tarafından, OT siber güvenlik yönetiminde çalışacak birim ve personelin, operasyon sahasında çalışan ekiplerin hayatını zorlaştıran kimselermiş gibi görünmesi yerine, mühendislik görevlerini kolaylaştıran ve operasyon personelini destekleyen unsurlar olarak tanınmaları sağlanmalıdır. OT ağ görünürlüğü yalnızca EKS güvenliği ve endüstriyel olaylara müdahale ile ilgili değildir. OT ağına özel görünürlüğün tüm avantajları bilinmeli, ekiplere ve tüm paydaşlara bildirilmeli ve bu tür teknoloji için muhakkak bütçe planlanmalıdır.

Taktiksel Hareket

Hem OT-ağının diğer ağlara entegre olduğu trafiğin (Kuzey/Güney) hem de dahili OT-ağ görünürlüğünü (Doğu/Batı) elde etme yolunda süreçlerin anlaşılması için ilgili mühendislik personeliyle birlikte çalışma yapılmalıdır. Trafik yakalamalarını elde etmek amacıyla sınır güvenlik duvarları, dahili güvenlik duvarları ve tüm ağda bulunan yönetilen anahtarlama cihazları veya trafik erişim noktaları Purdue Modeline uygun olarak tanımlanmalı, buna uygun olarak ağ trafiğinin tamamını izleyebilecek tasarım yapılmalıdır.

SONUÇ

Yönetim kurulu seviyesindeki kritik altyapı sahiplerinin ve sahadaki operatörlerinin bir kuruluşu neyin kritik hale getirdiğini anlaması kritik önem taşıyor. Bu onların endüstriyel kontrol sistemleridir, yani OT/EKS sistemleri, mühendislik ve operasyonlardır.

OT mühendislik süreçleri tasarım sürecinden başlanarak güvenliğin ön planda tutulduğu bir projelendirme ile kurulmalıdır. Siber savunmanın yaşayan bir süreç olduğu ve saldırgan profillerinin sürekli kendini geliştirdiği de göz önüne alındığında, savunma stratejilerinin de sürekli gelişecek şekilde planlanması gerekmektedir.

Kanser hücresi sinsi bir zararlıdır. İlk hücrenin yıkıcı bir etkisinin olmadığını hepimiz biliyoruz. Ancak zaman içerisinde yayılan hücreler bir dokuyu, dokular ise organları yakıp yıkıyor. Siber saldırının da böyle etki yaptığı bilinmeli, erken teşhis ve tedavinin önemi burada da hissedilmelidir.

Yukarıdaki bulguların her biri endişe verici olsa da bu yazımızda, kritik altyapılarımızı korumanın gerçekçi eylemlerle mümkün olduğu anlatılmıştır. Çeşitli stratejik ve taktiksel hamlelerin yanı sıra eğitim ve geliştirme seçeneklerinin de değerlendirilmesi ile OT siber güvenlik modelinin olgunlaşması incelenmiş, okuyucuların daha somut gerçeklerle tehlikeyi fark etmeleri sağlanmıştır.