OT Sistemlerde Risk Yönetimi

Hakan Duran

Bu rapor, NIST SP800-82r3 raporu baz alınarak hazırlanmıştır. İngilizcede var olan kelimelerden security, bildiğimiz anlamda bir organizasyonu veya insanları tehditten koruma iken; safety, herhangi bir şeyi ona zarar verebilecek durumlardan yoksun etmek, selametinden emin olmaktır. Yazı boyunca security için güvenlik, safety için emniyet ifadesi kullanılmıştır.

Kuruluşlar; mali kayıplar, ekipman arızası ve personel güvenliği dahil olmak üzere iş hedeflerine ulaşırken her gün risklerle karşı karşıya gelir ve onları yönetmek zorunda kalırlar. Bu risklerin yönetilebilmesi adına risk yönetim süreçlerinin geliştirilmesi risklerin etkilerinin azaltılması için gereklidir. Bugüne dek risklerin azaltılması adına birçok framework geliştirilmiştir. OT sistemlerine sahip organizasyonlardaki risk yönetimi diğer alanlardaki risk yönetimlerine göre farklılık göstermektedir.

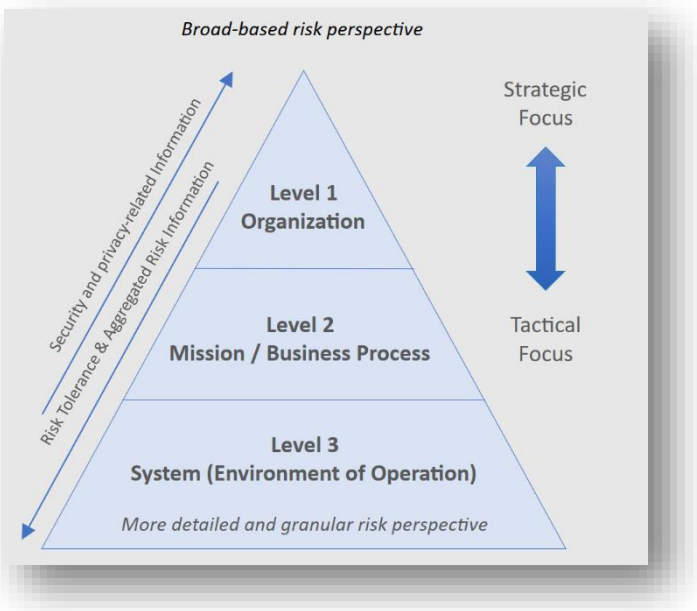
Organizasyonlardaki risk yönetim süreci üç katmanlı bir yapıdan oluşmaktadır. Bu katmanlar sırasıyla organizasyon katmanı, misyon ve iş süreci katmanı ve sistem katmanı (IT ve OT) olarak isimlendirilmiştir. Risk yönetim süreci bu üç katmanın birbirleriyle doğru iletişimi sağlanarak gerçekleştirilmektedir. Bu rapor, risk yönetim sürecinin OT tarafına daha çok odaklanarak hazırlanmıştır.

OT Güvenlik Risklerini Yönetmek

NIST SP 800-39 standardında belirtilmiş olan risk yönetim süreci bütün sistemlere uygulanabilmektedir. Ancak, bu standart OT sistemlerine uygulanırken belli farklar bulunmaktadır.

Risk yönetim süreci 4 adet bileşenden oluşmaktadır. Bunlar, riski çerçeve içine almak (framing risk), riskin değerlendirilmesi (assessing risk), riske cevap oluşturmak (responding to risk) ve riski izlemek (monitoring risk). Bu bileşenlerin uygulanması birbirine bağımlıdır ve organizasyon içerisinde eşzamanlı olarak gerçekleştirilebilir.

Üç katmanlı yapıya dayalı risk yönetim sürecinde Seviye 1, risk yönetimini organizasyonel perspektiften ele alır ve organizasyon içindeki tüm risk yönetimi faaliyetleri için içerik sağlayarak risk çerçevelemesini uygular. Seviye 2, riski misyon ve iş süreci perspektifinden ele alır ve Seviye 1 risk tarafından içerik, kararlar ve faaliyetler yönüyle bilgilendirilir. Seviye 3, sistem düzeyindeki riski ele alır ve Seviye 1 ve 2 faaliyetleri ve çıktıları tarafından bilgilendirilir.



OT Riskinin çerçevelenmesi (Risk Framing)

Çerçeveleme bileşeni, kuruluşların tutarlı risk yönetimi kararları alması için gerekli varsayımları, kısıtlamaları, risk toleranslarını ve risk yönetimi stratejilerini oluşturmaya yönelik süreçlerden oluşur. Risk çerçeveleme, kuruluşun tüm IT ve OT sistemlerine yönelik riski nasıl değerlendirmeyi, yanıtlamayı ve izlemeyi planladığını belirlemek için kurumsal yönetim yapısından, yasal/düzenleyici ortamdan ve diğer faktörlerden unsurları birleştirerek genel risk yönetimi stratejisini destekler.

OT sistemleri için emniyet, sistemlerin nasıl tasarlanıp çalıştırılacağına ilişkin kararları doğrudan etkiler. Emniyet, "ölüm, yaralanma, mesleki hastalık, ekipman veya mal hasarı/kaybı veya çevreye zarar verebilecek koşullardan korunmak" olarak tanımlanabilir. Buna dayanarak, insan emniyeti tipik olarak bir siber olaydan sonra OT sisteminin arızalanmasından kaynaklanabilecek yaralanma, hastalık veya ölüm derecesine göre değerlendirilir. Çalışanlar ve halkla ilgili daha önce gerçekleştirilen emniyet değerlendirmeleri dikkate alınır. Emniyetin önemi ve emniyet kültürünün geliştirilmesi, risk toleransının belirlenmesinde kritik bir rol oynar.

Kuruluşlar, emniyet açısından kritik her arıza durumunun veya bir tehlikeye yol açabilecek insan hatasının operasyonel davranışını sistematik olarak tahmin etmek veya tanımlamak için kapsamlı bir süreç kullanmayı düşünmek isteyebilir. Organizasyonlar ayrıca kendilerinde bulunan eski (legacy) sistem ve bileşenlere de yeni sistemlerin siber güvenliğine dikkat ettikleri kadar umursamalıdırlar.

OT sistemi operatörleri için bir diğer önemli endişe ise OT sistemi tarafından sağlanan hizmetlerin kullanılabilirliğidir. OT sistemi, sürekli ve güvenilir operasyonlara önemli bir ihtiyaç duyulan kritik altyapının (örn. su veya güç sistemleri) bir parçası olabilir. OT sistemlerinin kullanılabilirlik (availability) veya kurtarma (recovery) konusunda katı gereksinimleri olabilir. Bu hususların dikkate alınması, kuruluşların, sağlanan hizmetlere bağımlı olanlar üzerinde istenmeyen sonuçlardan kaçınacak risk kararları almasına yardımcı olacaktır. Daha spesifik olarak kuruluşlar, sistem kullanılabilirliğini tehdit eden siber güvenlik riskleri oluşturan birbirine bağımlı OT sistemlerini tanımlamayı düşünmelidir. Bu gibi durumlarda bir sistemde gelen kaza, bağlı olan diğer sistemleri ve bileşenleri etkileyebilir. Bu sistem ve bileşenler organizasyonun içerisinde veya dışarısında olabilir, kazanın yayılması fiziksel veya mantıksal sebeplerden kaynaklanabilir.

Amerika Birleşik Devletleri'nde Cybersecurity and Infrastructure Security Agency (CISA), hükumet ve endüstri arasında ulusal seviyede OT risklerini yönetmede sorumlu bileşendir. CISA, güvenlik açıklarını tespit etmek ve OT sistemlerinin siber güvenlik duruşunu güçlendiren sağlam, proaktif azaltma stratejileri geliştirmek için tüm kritik altyapı sektörlerindeki OT sistem satıcılarına ve varlık sahiplerine, operatörlere ve diğer satıcılara yardımcı olur.

Kuruluşlar, görev ve OT sistemlerine yönelik riskleri değerlendirmek için NIST Ulusal Güvenlik Açığı Veritabanı (NVD) ve Endüstriyel Kontrol Sistemleri (ICS) için MITRE ATT&CK çerçevesi gibi kaynakları kendi süreçlerine dahil etmeyi düşünebilir.

Risk çerçevesinin bir parçası olarak kuruluşların aşağıdakileri de dikkate alması gerekebilir:

• Organizasyon genelinde riskin nasıl değerlendirildiği, yanıtlandığı ve izlendiğiyle ilgili varsayımlar

• Kuruluşun risk toleransı, stratejik amaç ve hedeflere ulaşmanın bir parçası olarak kabul edilebilecek risk düzeyi

Bu süreçler, kuruluşların, OT hususlarını da içeren etkilerin değerlendirilmesi için ortak bir çerçeve belirlemesini gerektirebilir. Yaklaşımlardan biri, sistemlerin gizlilik, bütünlük ve kullanılabilirlik (Confidentiality, Integrity, Accessibility) güvenlik hedefleri açısından düşük etkili, orta etkili veya yüksek etkili olarak kategorize edildiğini belirten NIST FIPS 199'a [FIPS199] dayanmaktadır. ISA 62443-3-2'ye [ISA62443] dayanan başka bir yaklaşım, OT değerlendirilmesinde kullanılabilir. Aşağıdaki tablo, FIPS199 standardının OT sistemlerine uyarlanmasıyla elde edilmiştir.

Kategori	Yüksek etki	Orta etki	Düşük etki
Birden fazla yerde kesinti	Birden fazla tesisteki operasyonlarda önemli kesintiler yaşandı ve restorasyonun bir veya daha fazla gün sürmesi bekleniyor	Birden fazla tesisteki operasyonel kesintiler nedeniyle restorasyonun bir saatten fazla sürmesi bekleniyor	Birden fazla tesisteki operasyonların kısmen kesintiye uğraması ve tam kapasiteye restorasyonun bir saatten az sürmesi
Ulusal altyapı ve hizmetler	Birden fazla sektörü etkiliyor veya toplum hizmetlerini büyük ölçüde sekteye uğratıyor	Sektörü şirketin ötesinde etkileme potansiyeli	Bireysel şirketin ötesindeki sektörlere etkisi çok az veya hiç yok ve topluluk üzerinde çok az etkisi var veya hiç etkisi yok
Maliyet (Gelire bağlı olarak yüzde)	> %25	> %5	< %5
Yasal düzey	Faaliyet ruhsatını etkileyen ağır suç veya uyum ihlali	Para cezasıyla sonuçlanan kabahat cezai suç veya uyum ihlali	-
Kamu saygısı	Marka imajının kaybı	Müşteri güveninin kaybı	-
Site içerisindeki insanlar	Ölüm	İş günü kaybı veya ağır yaralanma	İlk yardım veya kaydedilebilir yaralanma
Site dışarısındaki insanlar	Ölüm veya büyük toplumsal olay	Şikayetler veya yerel topluluk etkisi	Şikayet yok
Çevre	Bölgesel sorumlu kurumun incelemesi veya geniş alanda uzun vadeli hasar	Yerel sorumlu kurumun incelemesi	Raporlanabilecek limitin altında hasar

Düşmanca (adversarial) tehditler için, meydana gelme olasılığının değerlendirilmesi genellikle düşmanın niyetine, yeteneğine ve hedeflemesine dayanır. Düşman tehdidi dışındaki olaylar için, gerçekleşme olasılığı, tarihsel kanıtlar, ampirik veriler ve diğer faktörler kullanılarak tahmin edilir. Kuruluşlar, minimum düzeyde kurumsal geçmiş veri bulunduğunu tespit ederse analizlerini, benzer kuruluşlar için rapor edilen siber güvenlik olaylarını açıklayan sektöre özgü verileri dikkate alacak şekilde genişletmeyi düşünebilirler. Tehdidin ortaya çıkma olasılığı aynı zamanda kuruluşun durumuna da bağlı olabilir (örneğin, temel misyon ve iş süreçleri, kurumsal mimari, bilgi güvenliği mimarisi, bilgi sistemleri ve bu sistemlerin çalıştığı ortamlar).

OT Riskinin Değerlendirilmesi (Risk Assessing)

Risk değerlendirmeleri, riskin çerçevelenmesinin çıktılarından (örneğin, kabul edilebilir risk değerlendirme metodolojileri, risk yönetimi stratejisi ve risk toleransı) yararlanır ve operasyonlara, varlıklara, bireylere ve diğer kuruluşlara yönelik riskleri belirler, tahmin eder ve önceliklendirir. Risk değerlendirmeleri tüm risk yönetimi düzeylerinde (yani organizasyon, misyon ve iş fonksiyonu ve sistem) gerçekleşir ve diğer düzeylerdeki risk değerlendirmelerine bilgi sağlamak için kullanılabilir. Risk değerlendirmesi hangi risk yönetimi seviyesinde yapılırsa yapılsın, riskin değerlendirilmesi, tehditlerin ve zayıf noktaların, bu tehdit ve güvenlik açıklarının neden olabileceği zararın ve bu tehdit ve güvenlik açıklarından olumsuz olayların ortaya çıkma olasılığının belirlenmesini gerektirir.

Risk değerlendirmeleri genellikle anlık raporlardır. Sonuç olarak kuruluşlar, güncel kaldıklarından ve güvenlik düzeyinin yeterli olduğundan emin olmalıdır. Kuruluşlar, OT ortamlarındaki aşağıdakiler gibi ortak güvenlik açığı alanlarını belirlemek amacıyla CISA'nın Uyarıları ve Önerileri, NIST'in NVD'si ve ICS için MITRE ATT&CK tarafından sağlanan bilgileri incelemek isteyebilir:

• Kötü kodlama uygulamaları, ağ tasarımları veya cihaz yapılandırmaları

• Savunmasız ağ hizmetleri ve protokolleri

• Zayıf kimlik doğrulama

• Aşırı ayrıcalıklar

• Bilgi ifşası

OT sistemleri genellikle belirli çevresel gereksinimlere sahiptir (örneğin, bir üretim prosesi kesin bir sıcaklık gerektirebilir) veya operasyonlar için fiziksel ortamlarına bağlı olabilirler. Kuruluşlar, ilgili risklerin tanımlanması için bu gereklilikleri ve kısıtlamaları çerçeveleme bileşenine dahil etmeyi düşünebilir. Ek olarak kuruluşlar şunları dikkate almak isteyebilir:

• Güvenlikle ve insan hayatıyla doğrudan ilgili olan fiziksel varlıkların ve güvenlik kontrollerinin belirlenmesi ve OT sisteminin operasyonlarının sürekliliğinin sağlanması

• OT sisteminin işlevselliğini tehdit edebilecek fiziksel varlıklarla ilişkili siber güvenlik risklerinin belirlenmesi

• Fiziksel güvenlik personelinin korudukları OT sistem ortamlarıyla ilişkili ilgili riskleri ve fiziksel güvenlik önlemlerini anlamasını sağlamak

• Fiziksel güvenlik personelinin, OT sistemi üretim ortamında veri toplamayı barındıran ve hassas alanlarda çalışan alanlardan haberdar olmasını sağlamak

• Fiziksel güvenliğin tehlikeye atılması durumunda acil müdahale planlarını belirleyerek iş sürekliliği risklerini azaltmak

Risk değerlendirmeleri aynı zamanda olumsuz olay etkilerini en aza indirmek için uygulanan dijital ve dijital olmayan mekanizmaların da gözden geçirilmesini gerektirir. OT sistemleri genellikle hata toleransı sağlamak ve OT'nin kabul edilebilir parametrelerin dışında hareket etmesini önlemek için dijital olmayan mekanizmalar içerir. Bu dijital olmayan mekanizmalar, dijital bir olayın OT üzerinde yaratabileceği ve risk değerlendirme sürecine dahil edilmesi gereken olumsuz etkilerin azaltılmasına yardımcı olabilir. Örneğin, OT genellikle güvenli bir sınırın dışında çalışmasını engelleyebilecek ve dolayısıyla bir saldırının etkisini sınırlayabilecek dijital olmayan kontrol mekanizmalarına sahiptir (örneğin, mekanik tahliye basınç valfi). Analog mekanizmalar (örn. sayaçlar, alarmlar) fiziksel sistem durumunu gözlemlemek ve dijital okumaların mevcut olmaması veya bozuk olması durumunda operatörlere güvenilir veriler sağlamak için de kullanılabilir.

Dijital olmayan kontrol mekanizmalarına analog görüntüleyiciler, alarmlar, manüel kontrol mekanizmaları ve analog kontrol mekanizmaları örnek verilebilir.

Analog görüntüleyiciler ve alarmlar: Fiziksel sistemin durumunu (örneğin sıcaklık, basınç, voltaj, akım) ölçer, görüntüler ve dijital ekranlar kullanılamadığında veya bozulduğunda operatöre doğru bilgiler sağlayabilir. Bilgi, operatöre bazı dijital olmayan ekranlarda (örneğin termometreler, basınç göstergeleri) ve sesli alarmlarla sağlanabilir.

Manüel kontrol mekanizmaları: Manuel kontrol mekanizmaları (ör. manuel valf kontrolleri, fiziksel kesici anahtarlar), operatörlerin dijital OT sistemine güvenmeden bir aktüatörü manuel olarak kontrol etmesine olanak tanır. Bu, OT sistemi kullanılamıyorsa veya tehlikede olsa bile aktüatörün kontrol edilebilmesini sağlar.

Analog kontrol mekanizmaları: Analog kontrol sistemleri, fiziksel bir süreci izlemek ve kontrol etmek için dijital olmayan sensörler ve aktüatörler kullanır. Bunlar, dijital OT sistemi kullanılamadığında veya bozulduğunda fiziksel sürecin istenmeyen bir duruma girmesini önleyebilir. Analog kontroller regülatörler ve elektromekanik röleler gibi cihazları içerir. Buna bir örnek, acil durumlarda veya anormal durumlarda, dahili sıvı basıncının belirli bir değerin üzerine çıkmasını önlemek ve böylece prosesi daha güvenli bir duruma getirmek için açılacak şekilde tasarlanmış bir cihazdır. Cihaz aynı zamanda bir basınç tahliye vanası, tekrar kapanmayan bir basınç tahliye cihazı (örneğin patlama diski) veya bir vakum tahliye vanası gibi aşırı dahili vakumu önleyecek şekilde de tasarlanabilir.

OT Riskine Cevap Oluşturulması

Risk yanıt bileşeni, riski ele almak için olası eylem planlarını belirleyerek, bu olasılıkları kuruluşun risk toleransını ve çerçeveleme sırasında belirlenen diğer konuları göz önünde bulundurup değerlendirdikten sonra en iyi alternatifi seçerek, risk çerçeveleme bileşenine uygun olarak riske kuruluş çapında bir yanıt sağlar. Müdahale bileşeni, tanımlanan riske yönelik seçilen eylem planının uygulanmasını içerir: kabul etme, kaçınma, hafifletme, paylaşma, aktarma veya bu seçeneklerin herhangi bir kombinasyonu. Bir OT sistemi için mevcut risk yanıtları, sistem gereksinimleri, operasyonlar üzerindeki potansiyel olumsuz etkiler ve hatta mevzuata uygunluk rejimleri tarafından kısıtlanabilir.

OT Riskinin İzlenmesi

Riskin izlenmesi, risk yönetimi faaliyetlerinin dördüncü bileşenidir. Kuruluşlar, seçilen risk yönetimi stratejilerinin uygulanması, risk hesaplamasını etkileyebilecek ortamdaki değişiklikler ve risk azaltma faaliyetlerinin etkinliği ve verimliliği de dahil olmak üzere riski sürekli olarak izler. İzleme bileşenindeki faaliyetler diğer tüm bileşenleri etkiler.

Birçok OT sistem izleme özelliği, sistem değişikliklerini tespit etmek için pasif izleme tekniklerinden yararlanır. Ancak bu her zaman sistemdeki tüm değişiklikleri kapsamayabilir. Daha fazla sistem bilgisine erişmek için yerel protokol iletişimlerinden yararlanan modern izleme platformları farkındalığı artırabilir ancak bu OT sistemlerinin sınırlamalarının anlaşılması gerekir. OT ortamıyla ilgili tehdit bilgileri gelişiyor ve bu tehdit bilgilerinin kullanılabilirliği ve doğruluğu henüz geliştirme aşamasında. Doğaları gereği tehditlerin geçmiş verilerle bile doğru bir şekilde tahmin edilmesi zor olabilir. Kuruluşlar, tehditleri gerçekleşme olasılığına ve potansiyel sonuçlarına göre sınıflandırmalıdır.

OT riskinin belirlenmesinde özel alanlar

OT için tedarik zincirinde risk yönetimi

Siber güvenlik riskleri, OT ihtiyaçlarını desteklemek için edinilen ürün veya hizmetlerden kaynaklanabilir. Bu riskler tedarik zincirinin herhangi bir yerinde ve yaşam döngüsünün herhangi bir aşamasında ortaya çıkabilir. Kötü niyetli, doğal veya kasıtsız olsun, bu riskler, kritik OT sistemleri ve bileşenlerinin kullanılabilirliği ve bütünlüğünün yanı sıra OT tarafından kullanılan verilerin kullanılabilirliği, bütünlüğü ve gizliliğinden ödün verme potansiyeline sahiptir. Birkaç istisna dışında, OT'den sorumlu kuruluşlar çeşitli ihtiyaçlar için tedarikçilere, diğer üçüncü taraf sağlayıcılara ve onların genişletilmiş tedarik zincirlerine güvenmektedir. Bu tedarik tarafı kuruluşları, teknoloji ürünlerinin üretimi ve tedariği, yazılım yükseltmeleri ve yamalarının sağlanması, entegrasyon hizmetlerinin gerçekleştirilmesi veya OT sistemlerinin, bileşenlerinin ve operasyonel ortamlarının günlük operasyonlarının ve bakımının desteklenmesi dahil olmak üzere kritik rolleri ve işlevleri yerine getirir. Bu nedenle OT kuruluşları, bu tedarik tarafı kuruluşlarından ve sağladıkları ürün ve hizmetlerden devralınabilecek tedarik zinciriyle ilgili riskleri anlamaya ve azaltmaya çalışmalıdır. Tedarik zincirlerindeki siber güvenlik risklerinin belirlenmesi, değerlendirilmesi ve bunlara etkili bir şekilde yanıt verilmesi, siber güvenlik tedarik zinciri risk yönetimi (Cybersecurity Supply Chain Risk Management) (C-SCRM) hususlarının kurumsal politikalara, planlara ve uygulamalara dahil edilmesiyle en iyi şekilde gerçekleştirilir. Bu, siber güvenlik beklentilerini ve gerekliliklerini satıcılara genişletmeyi ve satın alınan ürün ve hizmetlerle ilişkili tedarik zincirleri üzerinde daha iyi anlayış, görünürlük ve kontrol elde etmeyi içerir.

Kuruluşlar, tedarikçilerin ve hizmet sağlayıcıların yeteneklerini, güvenilirliklerini, iç güvenlik uygulamalarının yeterliliğini, koruma önlemlerinin etkinliğini, tedarik zinciri ilişkilerini ve bu ilişkiler ve bağımlılıklarla ilişkili olabilecek her türlü riski araştırmak için incelemelidir. Ayrıca, ürünün kullanım ömrü boyunca orijinal yedek parçalara veya güncellemelere ulaşmanın ne kadar zor olabileceği ve tedarik kaynaklarının ne kadar çeşitli olduğu ve gelecekte olabileceği konusu da özel olarak dikkate alınmalıdır.

OT organizasyonları tedarik zincirinden dolayı oluşabilecek riskleri yönetmek için NIST SP 800-161, Federal Bilgi Sistemleri ve Kuruluşları için Tedarik Zinciri Risk Yönetimi Uygulamaları, kılavuzundan yararlanabilirler.

Sistemlerin insan için emniyetini sağlamak

İngilizcede var olan kelimelerden security, bildiğimiz anlamda bir organizasyonu veya insanları tehditten koruma iken; safety, herhangi bir şeyi ona zarar verebilecek durumlardan korumak, selametinden emin olmaktır. Yazı boyunca security için güvenlik, safety için emniyet ifadesi kullanılmıştır.

Emniyet ve emniyet değerlendirmeleri kültürü, OT kullanıcı topluluğunun büyük bir bölümünde iyice yerleşmiştir. Emniyet değerlendirmeleri öncelikle fiziksel dünyayla ilgilenirken, bilgi güvenliği risk değerlendirmeleri dijital dünyayı dikkate alır. Ancak OT ortamında fiziksel ve dijital iç içe geçmiş durumdadır ve önemli ölçüde örtüşme meydana gelebilir. Bu nedenle kuruluşlar, bilgi güvenliği için risk değerlendirmeleri gerçekleştirirken güvenlik için risk yönetiminin tüm yönlerini (örneğin, risk çerçeveleme, risk toleransları) ve güvenlik değerlendirmesi sonuçlarını dikkate almalıdır. Bilgi güvenliği risk değerlendirmesinden sorumlu personel, emniyetle ilgili sonuçları olabilecek tanımlanmış riskleri tanımlayabilmeli ve iletebilmelidir.

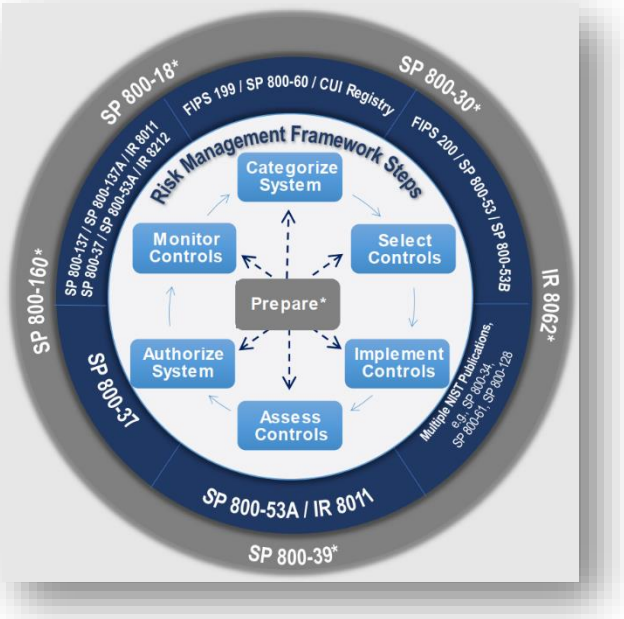
Emniyet sistemleri, bir siber olayın OT üzerindeki etkisini azaltabilir ve genellikle insanların, çevrenin, süreçlerin ve varlıkların emniyetini sağlamak için belirli izleme ve kontrol işlevlerini gerçekleştirmek üzere kullanılır. Bu sistemler geleneksel olarak tamamen yedekli ve birincil OT'den bağımsız olacak şekilde uygulansa da bazı mimariler kontrol ve emniyet işlevlerini, bileşenlerini veya ağlarını birleştirir. Kontrol ve emniyetin birleştirilmesi, OT'nin tehlikeye atılması durumunda gelişmiş bir saldırganın hem kontrol hem de emniyet sistemlerine erişmesine olanak tanıyabilir. Kuruluşlar, uzlaşma riskine uygun olarak bileşenlerin yeterli şekilde ayrılmasını sağlamalı ve uygulanan güvenlik kontrollerinin, sistemi olumsuz etkileyip etkilemediğini belirlemek için emniyet sistemi üzerindeki etkisini değerlendirmelidir.

NIST Risk Management Framework

https://csrc.nist.gov/projects/risk-management

NIST Risk Yönetimi Çerçevesi (RMF), herhangi bir kuruluşun bilgi güvenliği ve gizlilik riskini yönetmek için kullanabileceği kapsamlı, esnek, tekrarlanabilir ve ölçülebilir 7 adımlı bir süreç sağlar. NIST RMF, Federal Bilgi Güvenliği Modernizasyon Yasası'nın (FISMA) gerekliliklerini karşılamak için risk yönetimi programlarının uygulanması için bir kılavuz işlevi görür.

RMF, 7 bileşenden oluşur. Sonraki başlıklarda RMF'in OT'ye nasıl uygulanabileceği her bileşen için ayrı ayrı incelenecektir.



Hazırlık (Prepare)

Amaç: Hazırlık adımının amacı, kuruluşun RMF'yi kullanarak güvenlik ve gizlilik risklerini yönetmesine yardımcı olmak için organizasyonel, misyon ve iş süreci ile sistem düzeylerinde temel faaliyetleri yürütmektir. Hazırlama adımı, risk yönetimini desteklemek için kuruluş çapında yönetişim ve kaynakların mevcut olmasının önemini vurgulamak amacıyla siber güvenlik programları kapsamında hâlihazırda yürütülmekte olan faaliyetlerden yararlanır.

Beklenen sonuçlar:

- Temel risk yönetimi rolleri belirlendi.
- Kurumsal risk yönetimi stratejisi oluşturuldu, risk toleransı belirlendi.
- Kuruluş çapında risk değerlendirmesi.
- Sürekli izlemeye yönelik kuruluş çapında bir stratejinin geliştirilmesi ve uygulanması.
- Ortak kontroller belirlendi.

Kategorizasyon (Categorize)

Amaç: Sistemlerin ve bu sistemler tarafından işlenen, saklanan ve iletilen bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin kaybıyla ilgili olumsuz etkiyi belirleyerek kurumsal risk yönetimi süreçlerini ve görevlerini bilgilendirme aşamasıdır.

Beklenen sonuçlar:

• Belgelenen sistem özellikleri

• Sistemin güvenlik sınıflandırması ve tamamlanan bilgiler

• Kategorizasyon kararının yetkili yetkili tarafından gözden geçirilmesi/onaylanması

Kategorizasyon adımında bilgi ve sistemin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin kaybının olası olumsuz etkileri belirlenir. Göz önünde bulundurulan her bilgi türü ve sistem için, üç güvenlik hedefi (gizlilik, bütünlük ve kullanılabilirlik) bir güvenlik ihlalinin üç potansiyel etki seviyesinden (düşük, orta, yüksek) biriyle ilişkilidir. Üç güvenlik hedefi arasında kullanılabilirlik genellikle bir OT için en büyük endişe kaynağıdır. Bu sınıflandırma sürecine ilişkin standartlar ve kılavuzlar sırasıyla FIPS 199 ve NIST SP 800-60'da bulunabilir.

Seçim (Select)

Güvenlik kontrolleri, sistemin ve bilgilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için bir kurumsal sistem içinde kullanılan koruma önlemleri veya karşı önlemlerdir. **Gizlilik kontrolleri**, bir bireyi korumak, geçerli gizlilik gerekliliklerine uyumu sağlamak ve gizlilik risklerini yönetmek için bir kuruluş içinde kullanılan idari, teknik ve fiziksel korumalardır.

Amaç: Sistemi ve organizasyonu riskle orantılı olarak korumak için gerekli kontrolleri seçin, uyarlayın ve belgeleyin

Beklenen sonuçlar:

• seçilen ve uyarlanan kontrol temelleri

• sisteme özel, hibrit veya ortak olarak belirlenen kontroller

• belirli sistem bileşenlerine tahsis edilen kontroller

• sistem düzeyinde sürekli izleme stratejisi geliştirildi

• kontrol seçimini, tasarısını ve tahsisini yansıtan güvenlik ve gizlilik planları incelenir ve onaylanır

Kontroller, sisteme, sistem öğelerine ve çalışma ortamına tahsis edilen güvenlik ve gizlilik gereksinimlerine göre seçilir. Bu gereksinimlerin tahsisi Hazırlama adımında gerçekleştirilir.

Temel kontrol seçimi yaklaşımında "kontrol temelleri", bir grubun, kuruluşun veya ilgili topluluğun koruma ihtiyaçlarını karşılamak için özel olarak bir araya getirilmiş, önceden tanımlanmış kontrol kümeleridir. Kuruluş tarafından oluşturulan kontrol seçimi yaklaşımında kuruluş, kontrolleri seçmek için kendi seçim sürecini kullanır. Bu, sistemin oldukça uzmanlaşmış olduğu (örneğin bir silah sistemi veya tıbbi cihaz) veya sınırlı bir amacı veya kapsamı olduğu (örneğin bir akıllı sayaç) durumlarda gerekli olabilir.

Seçim adımının amacı, sistemi riskle orantılı olarak korumak için başlangıç kontrollerini seçmektir. Kontrol temelleri, kontrol seçim sürecinin başlangıç noktasıdır ve Kategorizasyon adımında tanımlanan sistemlerin güvenlik kategorisine ve ilgili etki düzeyine göre seçilir. NIST SP 800-53B [SP800-53B] federal sistemler ve bilgiler için önerilen kontrol temellerini tanımlar.

Sistemler ve organizasyonlar için topluluk çapında ve özel kontrol setleri geliştirme ihtiyacını karşılamak amacıyla **örtü** kavramı tanıtıldı. Örtü, NIST SP 800-53B, Ek C'de açıklanan güvenlik kontrolü temel hatlarına yönelik kılavuzun uygulanmasından elde edilen, tamamen belirlenmiş bir dizi kontrol, kontrol geliştirmeleri ve tamamlayıcı kılavuzdur.

Uygulama (Implement)

Amaç: Sistem ve organizasyon için güvenlik ve gizlilik planlarındaki kontrolleri uygulamak

Beklenen sonuçlar:

- Uygulanan güvenlik ve gizlilik planlarında belirtilen kontroller
- Uygulanan kontrolleri yansıtacak şekilde güncellenen güvenlik ve gizlilik planları

Uygulama adımı, kontrollerin yeni veya eski sistemlerde uygulanmasını içerir. Bu bölümde açıklanan kontrol seçimi süreci OT'ye iki açıdan uygulanabilir: yeni ve eski sistemler.

Yeni sistemler için, sistemler henüz mevcut olmadığından ve kuruluşlar ilk güvenlik kategorizasyonlarını yürüttüğünden; kontrol seçim süreci, gereksinimler üzerinden uygulanır. Sistemlere yönelik güvenlik planlarında yer alan kontrollerin, sistem geliştirme yaşam döngüsünün geliştirme ve uygulama aşamalarında sistemlere dahil edilmesi beklenmektedir.

Buna karşılık, eski sistemler için güvenlik kontrolü seçim süreci, kuruluşların sistemlerde önemli değişiklikler öngördüğü durumlarda (örneğin büyük yükseltmeler, değişiklikler veya dış kaynak kullanımı sırasında) uygulanır. Sistemler halihazırda mevcut olduğundan, kuruluşlar muhtemelen güvenlik kategorizasyonunu ve güvenlik kontrolü seçim süreçlerini tamamlamış, bunun sonucunda ilgili güvenlik

planlarında önceden üzerinde mutabakata varılan kontroller oluşturulmuş ve bu kontroller sistemler içerisinde uygulanmıştır.

Değerlendirme (Assess)

Amaç: Kontrollerin doğru şekilde uygulanıp uygulanmadığını, amaçlandığı gibi çalışıp çalışmadığını ve sistem ve kuruluş için güvenlik ve gizlilik gereksinimlerini karşılama açısından istenen sonucu üretip üretmediğini belirlemek.

Beklenen sonuçlar:

- Değerlendirici/değerlendirme ekibi seçildi
- Güvenlik ve gizlilik değerlendirme planları geliştirildi
- Değerlendirme planları gözden geçirilir ve onaylanır
- Değerlendirme planlarına uygun olarak yürütülen kontrol değerlendirmeleri
- Güvenlik ve gizlilik değerlendirme raporları geliştirildi
- Kontrollerdeki eksiklikleri gidermek için iyileştirici eylemler gerçekleştirilir
- Güvenlik ve gizlilik planları, değerlendirmelere ve iyileştirme eylemlerine dayalı olarak kontrol uygulama değişikliklerini yansıtacak şekilde güncellenir

RMF'nin Değerlendirme adımı, sistemdeki kontrollerin uygulanmasında ve istenen sonuçları üretmede ne ölçüde etkili olduğunu belirler. NIST SP 800-53A, NIST SP 800-53'ten seçilen kontrollerin doğru bir şekilde uygulandıklarından, amaçlandığı gibi çalıştıklarından ve sistemin güvenlik gereksinimlerini karşılama açısından istenen sonucu ürettiklerinden emin olmak için değerlendirilmesine yönelik rehberlik sağlar.

Yetkilendirme (Authorize)

Amaç: Üst düzey bir yetkilinin, bir sistemin işleyişine veya ortak kontrollerin kullanımına dayalı güvenlik ve gizlilik riskinin kabul edilebilir olup olmadığını belirlemesini talep ederek hesap verebilirliği sağlamak.

Beklenen sonuçlar:

- Yetkilendirme sürecinin tamamlanması (yönetici özeti, sistem güvenliği ve gizlilik planı, değerlendirme raporu/raporları, eylem planı)
- Sistem veya ortak kontroller için yetkilendirme onaylanır veya reddedilir.

Yetkilendirme adımı, bir sistemin işleyişine yetki verilmesine ve üzerinde anlaşmaya varılan bir dizi kontrollerin uygulanmasına dayalı olarak operasyonlara, varlıklara ve bireylere yönelik risklerin açıkça kabul edilmesine yönelik bir yönetim kararını içerir. Sistem yetkilendirilmeden yeni bir sistem üretime veya işletmeye alınamaz.

Gözlem (Monitor)

Amaç: Risk yönetimi kararlarını desteklemek için sistem ve organizasyonun güvenlik ve gizlilik duruşu hakkında sürekli durumsal farkındalığı sürdürmek

Beklenen sonuçlar:

- Sürekli izleme stratejisine uygun olarak izlenen sistem ve çalışma ortamı

- Sürekli izleme stratejisine uygun olarak yürütülen kontrol etkinliğinin sürekli değerlendirmeleri
- Sürekli izleme faaliyetlerinin sonuçları kullanılarak yürütülen devam eden yetkilendirmeler

İzleme adımı, sistemdeki kontrolleri etkileyebilecek değişiklikleri sürekli olarak izler ve kontrol etkinliğini değerlendirir. NIST SP 800-37, Rev. 2, siber güvenliğin sürekli izlenmesine ilişkin rehberlik sağlar.

NIST RMF'in OT Sistemlerine Uygulanması

OT sistemlerinin risk değerlendirmesinde olabilecek aşamalar ve yapılabilecek uygulamalar aşağıda listelenmiştir.

Hazırlık

- Hem BT hem de OT sistemleri için personel siber güvenlik rollerini ve sorumluluklarını oluşturun ve sürdürün. Üçüncü taraf sağlayıcıların siber güvenlik rollerini ve sorumluluklarını dahil edin. OT personeline örnek olarak Proses/Tesis Yöneticisi, Proses Kontrol Mühendisi, Operatör, Fonksiyonel Güvenlik Mühendisi, Bakım Personeli ve Proses Güvenliği Yöneticisi verilebilir.
- Görev ve iş ihtiyaçlarını, benzersiz işletim ortamlarını ve/veya diğer gereksinimleri karşılamak üzere OT sistemleri için organizasyonel olarak uyarlanmış bir kontrol temeli geliştirilebilir.
- Kurumsal sistemler tarafından devralınabilecek ortak kontroller tanımlanır, belgelenir ve yayınlanır.
- Aynı etki düzeyine sahip organizasyonel sistemlerin önceliklendirilmesi yapılabilir. Etki düzeyinde önceliklendirmede güvenlik veya kritik hizmet sunumu gibi kriterler kullanılabilir.
- Paydaş varlıkları belirlenir ve önceliklendirilir. OT sistem bileşenleri arasında PLC'ler, sensörler, aktüatörler, robotlar, takım tezgahları, donanım yazılımı, ağ anahtarları, yönlendiriciler, güç kaynakları ve diğer ağ bağlantılı bileşenler veya cihazlar bulunabilir.
- Sistem düzeyinde bir risk değerlendirmesi tamamlanabilir veya mevcut bir risk değerlendirmesi güncellenebilir. Performans/yük testi ve sızma testi de dahil olmak üzere risk değerlendirmeleri, OT operasyonlarının test sürecinden olumsuz etkilenmemesini sağlamak için OT sistemlerinde dikkatle gerçekleştirilir.

Kategorizasyon

- Kuruluş tarafından tanımlanan bilgi türleri tarafından temsil edilen sistem tarafından işlenen bilgiler de dahil olmak üzere sistemin güvenlik sınıflandırması tamamlanır.
- Güvenlik sınıflandırması sonuçları güvenlik, gizlilik ve SCRM planlarında belgelenir.
- Güvenlik kategorizasyonu sonuçlarının kurumsal mimariyle ve kurumsal misyonları, iş fonksiyonlarını, misyon ve iş süreçlerini korumaya yönelik kararlılıkla tutarlı olması gerekir.
- Güvenlik kategorizasyonu sonuçları kuruluşun risk yönetimi stratejisini yansıtır.
- OT ve IT sistemleri farklı sınıflandırma kriterlerine sahip olabilir. Güvenlik sınıflandırması sırasında sistem bilgileri ve sistem süreci (örn. kimyasal üretim) dikkate alınmalıdır.

Seçim

- Kontroller, belirli kontrol temel çizgilerini oluşturacak şekilde uyarlanır. Operasyonel veya teknik kısıtlamalar nedeniyle belirli kontrollerin uygulanması mümkün olmayabilir. Kuruluşlar, riski kabul edilebilir bir düzeye kadar yönetmek için telafi edici kontrollerin kullanımını düşünmelidir.
- Benzersiz operasyonel, çevresel ve/veya kullanılabilirlik kısıtlamaları nedeniyle kontrol etkinliğini ölçmek için OT'ye özgü bir sürekli izleme stratejisi gerekli olabilir.

Uygulama

- Güvenlik ve gizlilik planlarında belirtilen kontroller uygulanır. Sistem güvenliği ve gizlilik mühendisliği metodolojileri, sistem güvenliği ve gizlilik planlarındaki kontrolleri uygulamak için kullanılır. Mevcut (operasyonel) OT sistemleri için kontrol uygulaması gerçekleştirilebilir. Kontrollerin OT sisteminin performansını ve güvenliğini etkilemediğinden veya bozmadığından emin olmak için tam bir doğrulama yapılması önerilir. Bazı durumlarda planlama sorunları nedeniyle riski hemen azaltmak mümkün olmayabilir. Ancak, geçici telafi edici kontrollerden yararlanılabilir.
- Planlanan kontrollerin uygulanmasındaki değişiklikler belgelenir. Kontrollerin uygulanması sırasında elde edilen bilgiler doğrultusunda güvenlik ve gizlilik planları güncellenmektedir.

Değerlendirme

- Kontrol değerlendirmelerini yürütmek üzere bir değerlendirici veya değerlendirme ekibi seçilir. Seçilen değerlendirici veya değerlendirme ekibi için uygun düzeyde bağımsızlık sağlanır. OT sistem personeli ve operatörü değerlendirme ekibine dahil edilebilir.
- Kontrol değerlendirmeleri güvenlik ve gizlilik değerlendirme planlarına uygun olarak gerçekleştirilir. Çalışmakta olan OT üzerindeki etkiyi azaltmak için masa üstü alıştırmaların veya simülasyonların kullanımı düşünülebilir. OT sisteminin test sürecinden olumsuz etkilenmemesini sağlamak amacıyla değerlendirmeleri dikkatli bir şekilde yürütmek için otomatik araçlar kullanılabilir.
- Sistemde ve operasyon ortamında uygulanan kontrollerdeki eksiklikleri gidermeye yönelik iyileştirici aksiyonlar alınır. Güvenlik ve gizlilik planları, değerlendirmelere ve sonraki iyileştirme eylemlerine dayalı olarak yapılan kontrol uygulama değişikliklerini yansıtacak şekilde güncellenir. İyileştirme eylemlerinin OT'nin verimliliğini ve güvenli operasyonlarını olumsuz etkilemediğinden emin olun. İyileştirme eylemlerinden biri olarak "telafi edici kontrol"lerin kullanımı düşünülebilir.
- Kabul edilemez risklere yönelik iyileştirme planlarını detaylandıran bir eylem planı, güvenlik ve gizlilik değerlendirme raporlarında belirlenebilir. Eylem planında OT sisteminin benzersiz zaman kısıtlamaları dikkate alınmalı ve OT sisteminin planlı program bakımı veya kapatılması da dikkate alınmalıdır.

Yetkilendirme

- Sisteme veya ortak kontrollere ilişkin yetkilendirme onaylanır veya reddedilir. Kuruluşların, sistem riskleri kabul edilebilir aralığın dışına çıktığında, bir sistemi veya bileşeni düzeltilene kadar çevrimdışına alamama gibi OT'ye özgü bağımlılıkları göz önünde bulundurarak iyileştirme stratejilerini belirlemeleri gerekebilir.

- Yetkilendirme kararları, önemli güvenlik açıkları ve riskler kuruluş yetkililerine raporlanır. Kararların, güvenlik açıklarının ve risklerin OT ve operasyon personeline bildirildiğinden emin olun.

Gözlem

- Performans etkilerini ve güvenlik sistemlerini kritik olarak değerlendiren OT'ye özgü sürekli izleme stratejisinden yararlanın.
- Sistem performansını ve güvenlik etkilerini dikkate alan sürekli değerlendirmeler gerçekleştirin.
- OT sistemi üzerindeki olayın etkisine ilişkin bir perspektif elde etmek için tespit edilen olay bilgilerini risk değerlendirme sonuçlarıyla ilişkilendirin.
- Sürdürülmesi gereken OT bileşenlerinin bakım ve onarımını göz önünde bulundurun.