Bilgi Güvenliğinin Temininde Askerî Yaklaşımlar - Alarm Seviyesi Yaklaşımı

İsmail Burak Tuğrul, CISSP[1]

[1] PwC Türkiye, Risk, Süreç ve Teknoloji Hizmetleri, İstanbul

buraktugrul@gmail.com

Özet: Bilgi güvenliğinin temininde kullanılabilecek bir askerî yaklaşım olan alarm seviyesi yaklaşımı, kurumların bilgi güvenliği problemlerinin yönetimine yeni bir bakış açısı getirmektedir. Bu bakış açısıyla, askerî birliklerin çeşitli tehditlere karşı kendilerini ya da sorumlu oldukları varlıkları korumak – kollamak amacıyla kullandığı alarm seviyelerinin bilgi güvenliği probleminin yönetilmesine nasıl uyarlanabileceğine ilişkin öneriler getirilmektedir. İfade edilen farklı alarm seviyelerinde atılacak farklı adımlarla, bilgi güvenliği probleminin yönetimine ayrılacak kaynakların etkin ve etkili bir şekilde uygulanmasının sağlanması hedeflenmektedir.

Anahtar Sözcükler: Bilgi Güvenliği, Siber Güvenlik, Siber Savunma, Siber Operasyonlar

Military-Based Approaches in Governing Information Security – Alarm Condition Approach

Abstract: Alarm condition approach, which is a military-based approach that can be used in governing information security, urges a new perspective for corporations to manage information security problem. With this approach new recommendations, which adapts military-based alarm condition system that is used to protect themselves or assets they are resposible for, is taken place. Main purpose, by taking different actions at different alarm conditions, is using the sources that are being used managing information security problem efficiently and effectively.

Keywords: Information Security, Cyber Security, Cyber Defence, Cyber Operations

1. Genel Bakış

Bilgi güvenliğinin sağlanabilmesi için kurumların aldığı birtakım önlemler mevcuttur. Bu önlemlerin bir kısmını klasik BT yaklaşımından evrilen çözümler olarak değerlendirebiliriz. Örneğin bilgi güvenliğinin bu kadar ön plânda olmadığı ilk zamanlarda kullanılan kimi ağ cihazları, hâlen sistemlerde yer almakta ancak bu ağ cihazlarının güvenlik özellikleri eskisine göre daha nitelikli bir hâl almaktadır.

Alınan önlemler ve getirilen yeni özellikler nasıl ki gelişim gösteriyorsa, yapılan saldırılar da aynı nisbette gelişmekte ve çeşitlenmektedir. Her ne kadar kurumların sürekli olarak her an bir siber saldırıya maruz kalabilecekleri düşüncesiyle adım atmaları gerekiyorsa da, bu adımları atarken mevcut şartları değerlendiren dinamik bir yapı kurmaları ve uygun kararları vermeleri, bilgi güvenliğinin etkin bir şekilde sağlanmasını oldukça kolaylaştıracaktır.

Örneğin devlet kurumlarını gözönünde bulunduralım. Bu kurumların varlıkları her zaman için saldırı tehdidi altındadır ancak bu tehdidin seviyesi her zaman için aynı mıdır? Mesela Türkiye için 30 Ağustos haftası ile 30 Ocak haftası aynı önemde midir? Bir tanesi devletin tarihinde önemli bir yere sahip olan Zafer Haftası'dır, diğeri ise sıradan bir hafta. Dolayısıyla salt bu unsuru düşündüğümüzde, hangi haftada devlet kurumlarının saldırıya uğrama ihtimalini daha yüksek olarak değerlendirmek mümkündür? Tabiî ki 30 Ağustos haftası. Saldırganların hiçbir motivasyon kaynağı olmasa bile sırf psikolojik olarak kazanım elde edebilmek için bile 30 Ağustos haftası daha mühimdir.

Bu örnekle varmak istediğimiz nokta şudur: Kurumlar bilgi güvenliğini sağlarken, bazı şartları gözönünde bulundurmalı, saldırıya maruz kalma olasılıklarının seviyesini bu şartlara göre değerlendirmeli ve bu seviyelere uygun aksiyon almalıdır. Bu ifadenin en bariz örneği, konumuzun başlığında da geçen askerî birliklerin uyguladığı yöntemdir.

Askerî birlikler, düşman unsurlardan gelecek saldırılara karşı çeşitli alarm seviyeleri belirlemişlerdir. Bu seviyeler her birliğin kendine özgü olabileceği gibi topyekûn o ülke silâhlı kuvvetlerine de ait olabilir. Bu seviyeler belirlendikten sonra ilgili birlik, kendisine göre hangi aksiyonları alması gerekiyorsa alır. Alarm seviyesi duruma göre yükseltilir veya düşürülür yani dinamik bir yapısı vardır. Birlikler sürekli teyakkuz hâlinde değildir.

Kurumlar bilgi güvenliğini sağlarlarken, bu tür bir askerî yaklaşımdan faydalanarak daha etkin ve daha etkili bir savunma mekanizması kurabilirler. Böylelikle hem daha başarılı savunmalar yapılarak daha müspet sonuçlar alınabileceği gibi, bu iş için ayrılan kaynaklar da daha verimli bir şekilde kullanılabilir. İlerleyen bölümlerde bilgi güvenliğine ilişkin savunma mekanizmasının nasıl dinamik bir yapıya kavuşturulabileceğine ve hangi seviyede hangi önlemlerin alınabileceğine ilişkin çözüm önerileri bulunmaktadır.

2. Alarm Seviyelerinin Tanımlanması

Alınacak aksiyonlardan önce, kurumların kullanacağı alarm seviyelerinin tanımlanması gerekmektedir. Alarm seviyeleri her kurumun kendisine has bir nitelik taşıyabilir. Kurumlar, yaptıkları işin büyüklüğü ve mahiyetine göre daha az ya da daha fazla sayıda alarm seviyesi tanımlayabilir. Kurumlar seviyeleri tanımlarken bu yazıyı bir referans olarak kullanabilir.

Bilgi güvenliği alarm seviyesi yaklaşımında, 4 farklı seviye kullanılabilir. Bunlar;

1. Yeşil Alarm Seviyesi – Düşük saldırı olasılığı
2. Mavi Alarm Seviyesi – Muhtemel saldırı olasılığı
3. Sarı Alarm Seviyesi – Yüksek saldırı olasılığı
4. Kırmızı Alarm Seviyesi – Her an yaşanabilecek saldırı olasılığı

3. Hangi Seviyede Olunduğunun Belirlenmesi

Kurumlar, mevcut durumlarının hangi alarm seviyesinde olduğunu belirlemek için çeşitli değişkenleri biraraya getirerek karar vermelidir. Bu aşamada formüle edilmiş bir yaklaşım kullanılabileceği gibi, aşağıda belirtilen örnek durumlar değerlendirilerek kantitatif bir tespit de yapılabilir. Seviyenin belirlenmesinde aşağıdaki doneler kullanılabilir:

- Benzer firmalara yönelik saldırıların / saldırı girişimlerinin gözetilmesi ve değerlendirilmesi
- Kurulan honeypot'lara yönelik saldırı girişimlerinin tespit edilmesi
- İşten kritik personel(ler)in ayrılması
- Spam'e takılan e-posta iletilerinin değerlendirilmesi
- Güvenlik firmalarının ilân ettiği güvenlik durumlarının izlenmesi(Symantec, Homeland Security vb.)
- Veri sızmasının tespiti
- Ağ taraması uyarıları, ağdaki anomaliler
- Yeni çıkan bir güvenlik açığının durumu - yayınlanmış sömürü(exploit) kodlarının bulunup bulunmadığı
- Sistemlerin ele geçirilmesi(Ele geçirilen sistemin ağdaki konumu ve kritikliği)
- Çalışan servislerde aksaklık / durma(Kritikliğine ve etkisine bağlı olarak)
- Hizmet kesintileri yaşanması(Kesintinin sıklığı / kesintinin yaşandığı sistemin kritikliği / kesinti sebebi)
- Yetkili kişilerin belirli / kısıtlı sistemlere erişememesi
- Ulusal kritik günler, sempozyumlar, konferanslar, anlaşmalar öncesi ve/veya sonrası
- Güvenlik bloglarında, forumlarında konuşulan konuların takibi

4. Alınacak Aksiyonlar

Yazının şimdiye kadar olan bölümlerinde, kullanılabilecek alarm seviyelerinin tanımlanmasından ve bu seviyelerin belirlenmesinde yararlanılabilecek verilerden bahsettik. Bu başlıkta ise, hangi seviyede ne tür bir aksiyon alınabileceği konusunda yol göstermeye çalışacağız. Daha önce de belirttiğimiz gibi alınacak aksiyonlar da kuruma özgü bir hüviyette olabilir ve çeşitlilik – farklılık arz edebilir. Seviyelerde önerilen aksiyonlar alınamayabileceği gibi uygulanabilir de olmayabilir. Buna ek olarak alt ya da üst seviyede önerilen adımlar, kurumun ilgili güvenlik seviyesiyle örtüşmeyebilir.

a) Yeşil Alarm Seviyesi – Düşük Saldırı Olasılığı

Bu seviye kurumun, düşük saldırı olasılığı sözkonusu olduğunda bulunacağı seviyedir. Saldırı ihtimali her zaman için var olmakla birlikte görülen, bilinen ya da duyumu alınan herhangi bir saldırı olasılığı bulunmamaktadır. Bu seviyede alınabilecek aksiyonlar:

- Farkındalığa yönelik ayda bir e-posta gönderilmesi
- IDS / IPS cihazlarının normal seyrinde çalışması
- Fiziksel güvenlik tedbirlerinin olağan şekilde devam etmesi
- Log kaynaklarının ayda bir gözden geçirilmesi
- Güvenlik yamalarının düzenli olarak geçilmesi
- Monitoring uygulanması
- Sızma testlerinin yaptırılması
- Sistem yedeklerinin belirlenen politikalar dahilinde alınmaya devam edilmesi
- İçerik filtreleme yazılımlarının belirlenen politikalar dahilinde çalışmaya devam etmesi

b) Mavi Alarm Seviyesi – Muhtemel Saldırı Olasılığı

Bu seviye, kurumun muhtemel bir saldırı riskiyle karşı karşıya olduğu durumda buluduğu seviyedir. Örneğin kullanılan sistemlere, teknolojilere ilişkin yeni güvenlik açıkları tespit edilmiş ancak bunlara ilişkin sömürü kodları yayınlanmamış olabilir. Veyahut takip edilen güvenlik sitelerinden bazı duyumlar, aynı sektördeki kurumlara yönelik saldırılar ya da içinde bulunulan ülkenin şartları sözkonusu olabilir. Bu seviyede alınabilecek aksiyonlar:

Önceki seviyede bulunan aksiyonların iyileştirilmesine yönelik adımlar:

- Farkındalığa yönelik iki haftada bir e-posta gönderilmesi
- IDS / IPS cihazlarının kurallarının kontrol edilmesi ve gerekli durumlarda sertleştirilmesi
- Fiziksel güvenlik tedbirlerinin artırılması – ör. devriye sayısının artırılması
- Log kaynaklarının iki haftada bir gözden geçirilmesi
- Güvenlik açığı tespit edilen servislerin, teknolojilerin yamanması
- Güvenlik açığı tespit edilen sistemlere daha fazla hassasiyet gösterilerek sızma testlerinin yapılması
- Yedekleme periyodunun mevcut politikalarda belirtilen süreden daha kısa süreye çekilmesi
- İçerik filtreleme yazılımlarına ilişkin kuralların gözden geçirilerek ihtiyaca göre yeniden düzenlenmesi

Bu seviyeye özgü olarak atılabilecek ek adımlar:

- Duruma göre yeni sistemlerin / ürünlerin / uygulamaların devreye alınma tarihlerinin yeniden gözden geçirilmesi ve/veya ertelenmesi
- Siber güvenlik tatbikat tarihlerinin tekrar gözden geçirilmesi ve/veya ertelenmesi

c) Sarı Alarm Seviyesi – Yüksek Saldırı Olasılığı

Bu seviye, kurumun yüksek olasılıkla saldırıya uğrama ihtimalinin olduğu durumlar için öngörülen seviyedir. Bu seviye için bir alt seviyedeki durumlara ek olarak kritik bir personelin işten ayrılması, kurumun kullandığı sistemlerde hâlihazırda sömürü kodları yayınlanan yeni güvenlik açıklarının bulunduğunun tespit edilmesi, veri sızmasının tespit edilmesi, ağ davranışlarında belirgin bir şekilde anomali gözlenmesi gibi durumlar sözkonusu olabilir. Bu seviyede alınabilecek aksiyonlar:

İkinci seviyedeki tedbirlere ek olarak;

- Erişim haklarının kontrol edilmesi
- Duruma göre mevcutta gerçekleştirilen testlerin durdurulması(sızma testi vb.)
- Güvenlik açığı bulunan uygulamaların / servislerin geçici bir süre kullanımının kısıtlanması ya da erişime kapatılması, açığın bulunduğu sisteme özgü önlemlerin alınması(sunucu, mobil cihaz, personel bilgisayarları vb.)
- VPN türü kuruma dışarıdan erişim yöntemlerinin kısıtlanması ya da devre dışı bırakılması(destek firma personeli de dahil olmak üzere)
- Personel izin günleri gözetilerek olası bir saldırıya müdahale edecek farklı birimlerdeki ekiplerden en az 1 kişinin, müdahale ekibi oluşturacak şekilde aksiyona hazır olmasının temini ve

gerektiği durumlarda ilgili kişilerin yıllık izinlerine ilişkin düzenlemeye gidilmesi

d) Kırmızı Alarm Seviyesi – Her An Gerçekleştirilebilecek Saldırı Olasılığı

Bu seviye, kurumun her an saldırıya uğrayabilme ihtimalinin olduğu durumlarda geçerlidir. Bir önceki seviyede belirtilen hâllere ek olarak çeşitli kaynaklardan kurumun saldırıya uğrayacağının tespit edilmesi, mantık bombası türü saldırılar tasarlanması, ağdaki belirgin bir saldırının öncülü olduğu kuvvetle muhtemel olan anomalilerin, sızmaların tespit edilmesi gibi durumlar sözkonusu olabilir.

Üçüncü seviyedeki önlemlere ek olarak;

- Geçerlilik süresinden bağımsız tüm kurum personelinin parola bilgisinin sıfırlanarak yeni parola oluşturulması
- Temizlik / bakım / diğer fizikî çalışmaların geçici süreyle ertelenmesi
- Tedarikçi firmalara kritik bilgi akışının kesilmesi - örn. müşteri bilgileri vb.
- Taşeron / destek firması personelinin geçici süreliğine kurum içine alınmaması / sistemlere erişiminin(VPN gibi) engellenmesi
- Dış bağlantıların kısıtlanması ya da kapatılması