

Bilgi savunmasının cepheleri

Fatih Emiral

Deloitte.

Etkin ve güçlü kurumlar için bilgi varlıkları (halen bilançolarında bu adla görülmeseler de) büyük değerlere ulaşmış ve vazgeçilmez konuma gelmiştir. Bu durumu reddetmek veya görmezden gelmek mümkün değildir. Değerli bir varlığa sahip olduğumuz ve bu varlığa yönelik tehditler de mevcut olduğunda, ihtiyatlı ve mantıklı varlık sahibinin yapması gereken, bu varlığı değeri nispetinde savunmasıdır.

Yani yapılacak savunma, yatırımının miktarı beklenen kayıp miktarına eşit veya daha az olmalıdır. Peki bilgi varlıklarımızı hangi cephelerde ve nasıl savunmalıyız? Eğer bilgi varlığımız etrafına geçilmez bir duvar örmek suretiyle korunabilseydi, çok basit bir çözüme kavuşmuş olurduk. Ancak bu pek olası bir strateji değildir çünkü pek çok varlığın aksine, "bilginin değeri doğru kişilerle ve doğru amaçlar için paylaşıldıkça ortaya çıkar ve artar". Bu durumda hat savunması yapılırsa bile belli durumlarda geçişe izin vermek, bilginin doğası nedeniyle gereklidir. Bilgi, merkezi depolarda, yedek depolarında, istemciler ve sunucularda bulunduğu gibi, istemci sunucu arasındaki veya sunucular arasındaki iletişim hatlarında yol alır, kağıt üzerine dökülür ve hatta kişilerin belleklerinde yer alır. Sonuç olarak hat ve alan savunmalarını bir arada kullanmak en doğru çözümdür. Çok kritik durumlarda, bire bir savunma dahi gerekebilir. Önemli olan bu savunma yöntemlerinin ortaya konması ve dengeli biçimde uygulanması, yani savunma yatırımlarının gerekli yerlere dengeli biçimde yapılmasıdır. Bilgi savunmasında kolektif olarak kullanılması gereken bu yöntemler aşağıdaki gibidir;

Güvenlik organizasyonu

Bilgi savunmasında, bilgiyi bilgi sahibinin isteği doğrultusunda kullanan ve bilgiden yarar gören herkes bir nefer olmalıdır. Ancak güvenlik organizasyonu daha aktif görevler üstlenmek üzere gereklidir. Böyle bir organizasyonun varlığı, bilgiye yönelik tehditlere karşı proaktif önlemler uygulanmasına imkan tanıyacaktır. Bilgi güvenliği organizasyonu; sürekli olarak tehditlerin belirlenmesi, risklerin analiz edilmesi, risklere karşı önlemlerin uygun olanlarının seçilmesi ve uygulanmasından sorumludur. Bu tür organizasyonların henüz pek görülmediği kurumlarımızda gözden kaçan zafiyetlerin doğması, kontrollerin dengeli uygulanmaması ve saldırılara zamanında müdahale edilememesi son derece olasıdır.

Kullanıcı ve BT çözümleri üretenlerin bilgi güvenliği bilinci

Kullanıcı tarafından işlenmek ve kullanılmak üzere üretilen ve saklanan bilgi, en nihayet kullanıcının fiziksel olarak elleri üzerinde veya hafızasında bulunacaktır. Kullanıcılar, bilgi sahipleri tarafından kendilerine verilen çeşitli türlerde bilgi erişim anahtarlarını da taşımaktadır. Kullanıcılara bilgiye erişim araçları ve eriştikleri bilgiyi neden ve nasıl korumaları gerektiği anlatılmalıdır. Kurum tarafından koyulan güvenli erişim ve kullanım kurallarına uymamanın somut ve etkili yaptırımları kullanıcılara iletilmelidir. Bu iletişim kullanıcı profil ve kültürüne göre şekillendirilmeli, hedefine ulaşabilmesi için, kullanıcının samimi iş birliğini kazanmayı amaçlamalıdır.

Güvenlik sistemlerinin mevcut bilgi sistemlerine sonradan eklenmesinin maliyeti, tasarım aşamasında sisteme dahil edilmelerinden çok daha yüksek olmaktadır. Ayrıca güvenlik açığı olan bilgi sistemlerinin üretimi, hem tespit maliyetini hem de (tespit ve düzeltme çabası olması kaydıyla) belli bir süre boyunca kurumun riskini artırmaktadır. Bu nedenle kurum yönetimi, fonksiyonel ihtiyaçlara odaklanmış ve zaman baskısı altında çalışan BT uzmanlarının güvenlik kontrollerini tasarım aşamasında, gerekiyorsa kontrol uzmanları ile birlikte belirlemeleri ve tasarımlarına eklemelerine önem vermeli ve bunun için imkan sağlamalıdır.

Kimlik yönetimi

Bilginin saklandığı ortam ve bilgiye erişim platformlarının artması, çok sayıda kullanıcı bilgisinin saklanması, dolayısı ile kullanıcılar tarafından çok sayıda kullanıcı kodu ve şifrenin hatırlanmasını zorunlu kılmıştır. Farklı ve çok sayıda giriş kontrol noktasının olması, kullanıcıların kolay şifre seçmesine, şifrelerini yazmasına, farklı platformlarda farklı şifre kriterlerinin uygulanmasına, işe başlayan, görevi değişen, işten ayrılan personel için operasyon yükünün artmasına veya ihmali ihtimalinin yükselmesine neden olmaktadır. Bu sorunu bertaraf etmek için, kimlik yönetimini tek noktaya toplayan standartlar ve araçlar geliştirilmiştir.

Uygulama güvenliği ve bütünlüğü

Uygulamalar ve diğer raporlama araçları, bilgi üretimi ve kullanımı için en önemli araçlardır. Bu araçlar iş süreçlerine uygun olarak tasarlanmakta, farklı kullanıcı profilleri için farklı ihtiyaçları yerine getiren modülleri barındırmaktadırlar. Uygulamalar, alt yapı güvenlik kontrolleri tarafından genellikle güvenilir varsayılır. Bu nedenle uygulamaların yetersiz kullanıcı tanıma ve erişim hakkı atama imkanlarının olması, uygulamalara erişim haklarının yeterli detayda tanımlanamaması, güvenlik kayıtlarının yeterince veya hiç tutulmaması, uygulama geliştirme ve değişim yönetiminde gerekli kontrollerin uygulanmaması gibi zafiyetler mevcutsa, uygulama araçları iç ve dış bilgi hırsızları ve saldırganlar için sonuna kadar açık kapılar haline gelebilirler. Uygulama kontrol alt yapılarındaki açıklar sadece teknik nedenlerden kaynaklanmaz. Kullanıcı haklarını tanımlama konusundaki prosedürel eksiklikler veya kurumun iş süreçlerinde rollerin ayrımı ilkelerinin uygulanmaması da kurumun uygulamalar aracılığı ile zarara uğratılmasına yol açabilir.

İnternet uygulamaları, kurum bilgi kaynaklarına açılan kapıyı daha geniş kitlelere ulaştırdıklarından, bu uygulamaların çalıştığı platformlara özgü ve genel uygulama zafiyetlerine özellikle dikkat edilmeli ve gerekli kontroller yapılmalıdır. Tüm uygulama geliştirme personelinin çalıştığı platformlarla ilgili güvenlik konularında bilgi sahibi olması gerekmekte, ancak İnternet uygulaması geliştiren personelin bu konuda çok daha yetkin olması büyük önem taşımaktadır.

Veri kalitesi

Kalite maliyeti bilindiği gibi alım, üretim ve satış sonrası aşamalarda oluşan test, kontrol, üretim kaybı, pazar kaybı ve garanti maliyeti gibi kalemlerden oluşur. Bilginin de üretilmesi için kaynak harcanır ve sonunda müşteriler tarafından kullanılır. Dolayısı ile bilgi de bir kalite maliyetine sahiptir. Veri kalitesindeki zafiyet doğrudan bilgiye karşı bir tehdit gibi görünmese de gerçekte yeterli bilginin oluşmasını engelleyerek, bilginin potansiyel değerini düşürür.

Veritabanı güvenliği

Günümüz veritabanı yönetim sistemleri, ayarlanabilir pek çok güvenlik parametresini bünyelerinde barındırmaktadır. Ancak tüm bilgi sistemleri gibi, kutudan çıktığı durumda veya yetersiz konfigürasyon ile kullanılan veritabanı yönetim sistemleri saldırılara açıktır. Veritabanları da tüm sistem yazılımları gibi, keşfedilmiş veya keşfedilmeyi bekleyen açıkları barındırmaktadırlar. Bilginin büyük zamanını geçirdiği ve topluca ulaşılabilirdiği bu ortamların korunması son derece önemlidir. Veritabanı güvenliğinde en kritik önlemlerden biri, veriye sadece uygulamalar aracılığı ile erişime izin verilmesidir. Tüm uygulamalar için olduğu gibi, hem BT personeli hem de son kullanıcılar için veritabanına doğrudan ulaşan uygulamaların (utility'ler) kurulumları, BT ve güvenlik yönetiminin kontrolünde, sadece ihtiyaç olması durumunda yapılmalıdır. Veritabanı profilleri için kullanılan şifreler kaba tahmin yöntemlerine dayanıklı karmaşıklık ve uzunlukta olmalı, düzenli veri yedekleri alınmalıdır.

İletişim güvenliği

İletişim giriş noktaları, fiziksel savunma hattından sonraki (veya önceki) ilk savunma noktalarıdır. İletişim güvenliğinde sadece bağlantı noktalarındaki fiziksel ve mantıksal kontroller yeterli değildir, iletişim hatlarının fiziksel güvenliği de önemlidir. İletişim güvenliğinin sağlanması kurum dışı iletişimde olduğu gibi, kurum içinde kritik alanlarda da gerekli olabilir. Günümüzde kablosuz iletişim teknolojisi de kullanılmaya başlandığından, fiziksel sınırlar önemini yitirebilmekte, bilgi ağının fiziksel güvenliğini anlamsız kılabilenmektedir. İletişim güvenliğinde gizlilik, bütünlük ve erişilebilirlik kriterlerinin hepsi tehdit edilebileceğinden, tüm kriterlerin yerine getirilmesi için gerekli kontrollerin uygulanması gereklidir. Gizlilik ve bütünlük ihtiyacı için kullanım alanına göre asimetrik veya simetrik şifreleme çözümleri uygulanmalı, sınır noktalarında sadece ihtiyaç

duyulan protokoller için ve mümkünse istenen noktalardan gelen giriş ve çıkış taleplerine izin verilmelidir. Erişilebilirliğe yönelik ve diğer tehditlerin hızlı algılanabilmesi için, kritik sunucular ve iletişim hatları üzerindeki iletişim paketlerini dinleyen saldırı tespit sistemleri kullanılmalı, güvenlik cihazlarının kayıtları izlenmelidir. İletişim güvenliğinde kullanılan giriş kontrol araçlarının, kritik sunucu ve dış dünyaya açılan sunucuların belirlenmiş açıkları kapanmış güncel versiyonlarının kullanılması hayati önem taşımaktadır. İçerideki bilgi kaynaklarının bulunduğu platformlara ilişkin dışarıya bilgi sızdırılmaması için gerekli kontrollerin uygulanması, dışarıya bilgi veren veya gereksiz bilgisayar servislerinin kapatılması da saldırganların muhtemel saldırılar için ihtiyaç duyacakları bilgiye ulaşmalarını zorlaştıracaktır.

Zayıflık denetimi

Kurumlar bilgi sistemleri alt yapılarında, çeşitli üretici firmalar tarafından üretilmiş sistem ve bilgi ağı yazılımlarını kullanmak zorundadırlar. Bu yazılımlar uygulama, veri ve iletişim platformlarını ve kurum sistemleri için alt yapı hizmetini sağladıklarından, bu sistemlere giriş bilgiye açılan kapı olabilir. Dünyanın her yerinde sistem yazılımlarının açıklarını keşfetmek için uğraşan pek çok kişi bulunmaktadır. Bu kişiler iyi veya kötü niyetlerle buldukları açıkları, İnternet üzerinden tüm dünya ile paylaşmaktadır. Yaklaşık olarak günde 20 sistem açığının İnternet üzerinden açıklandığı tahmin edilmektedir. Bilgi teknolojileri saldırılarının çok önemli bir bölümü, açıklanmış ve bilinen zayıflıklar kullanılarak gerçekleştirilmektedir. Bu nedenle kurumların bilgi sistemlerini saldırganlardan korumak için, kullanmakta oldukları sistemler ile ilgili açıkları yakından takip etmeleri, üretici firmalar tarafından geliştirilen çözümleri bir an önce uygulamaları çok önemlidir.

Virüs koruması

Virüs uygulamaları başka uygulamalara kendilerini ekleyerek, bu uygulamalar aracılığı ile veya doğrudan kendilerini bilgi ağı üzerindeki diğer sistemlere kopyalayarak çoğalırlar. Bu nedenle hem bilgi ağı hem de dosya dolaşımı (özellikle e-postalar aracılığı ile) kontrol edilmelidir. Çeşitli platformlar için geliştirilmiş anti-virüs yazılımları bulunmaktadır. En etkili yaklaşım; tüm bilgisayarlarda anti-virüs yazılımlarının bulunması, virüs imzalarının güncellenmesi, bilgi ağı giriş noktasında, e-posta sunucusu üzerinde ve kişisel bilgisayarlar üzerinde amaca özel uygun modüllerinin bulunması, anti-virüs uygulamalarının dosya kopyalama ve çalıştırma sırasında virüs kontrolü yapması, virüs tespiti üzerine sistem yöneticisini uyaracak biçimde ayarlanmış olması, BT yönetimi tarafından onay verilmeyen uygulamaların kurulumuna izin verilmemesi, uygulama kurulumunun BT kontrolünde olması, "worm" saldırılarını belirlemek için saldırı tespit ve koruma duvarı kullanılması, virüs tespiti durumunda virüs bulaşmış sistemlerin bilgi ağından izole edilmesi için gerekli prosedürlerin oluşturulması, mümkünse farklı katmanlarda farklı firmaların ürettiği anti-virüs yazılımlarının kullanılmasıdır.

Günlük tutma, izleme ve raporlama

Bilgi sistemlerine yönelik saldırılar genellikle kullanılan sistemlerin zayıflıklarından faydalanmak amacı ile saldırı öncesinde sistemlerin tanımlanmasını gerektirir. Bilgi sistemleri parametreleri ayarlanabilir kayıt özellikleri ile kendilerine yapılan talepleri, üzerlerinde gerçekleştirilen işlemleri kaydedebilir. Bilgi güvenliğine yönelik geliştirilmiş araçların kayıt yetenekleri daha da üstündür. Bu imkanlar sayesinde saldırı öncesi ve saldırı sırasında gerçekleştirilen faaliyetler kaydedilebilir. Kayıtlar saldırının gelişini haber verebilir veya başarılı saldırı sonrasında suç araştırmasında büyük fayda sağlar. Bu konuda kritik nokta, kayıtların tutulmasından daha çok, düzenli ve mümkünse otomatik olarak analiz edilmesidir. Aksi takdirde, sistem kaynağı ve disk kaybından başka bir işe yaramazlar.

Fiziksel güvenlik

Medeniyetimiz ne kadar gelişmiş olursa olsun, tüm tehditler karmaşık yöntemlerle ve bilgi ağları üzerinden gelmeyecektir. Bilgiye yönelik fiziksel tehditler, en az mantıksal tehditler kadar önemlidir. Fiziksel tehditler arasında çalınma, zarar verme, yetersiz ortamlar nedeniyle bilgi sistemlerinin zarar görmesi ve dolayısı ile bilgi teknolojileri hizmetlerinin kesintiye uğraması, donanım arızası ve bilginin sistemlerin yaydığı manyetik dalgaların dinlenmesi suretiyle çalınması sayılabilir. Fiziksel tehditlere karşı uygulanacak en etkili savunma yöntemleri olarak; periyodik fiziksel risk analizi, kritik donanımın periyodik bakımı, kritik bilgi sistemlerinin bulunduğu bölgelere sadece görevi gerektiren ve yönetim tarafından izin verilmiş kişilerin giriş çıkışına izin verilmesi, kritik bölgelerin izlenmesi, giriş-çıkışların kayıt altına alınması, kritik donanımın yangın,

su, nem, toz, ısı, elektrik kesintisi, manyetik alan ve statik elektriğe karşı yeterli önlemlerin alındığı ortamlarda saklanması sayılabilir.

İş sürekliliği ve felaket kurtarma

Fiziksel güvenlikle yakından ilgisi bulunan bu alan, kesintilere karşı iş süreçleri ve teknik alt yapı konusunda yapılacak planlama, eğitim ve testleri kapsar. Özellikle büyük ve karmaşık iş süreçlerine sahip kurumların bilgi teknolojileri bağımlılığı artmış, bu durum BT hizmetlerinin kesintisini daha kritik öneme kavuşturmuştur. İş sürekliliği ve felaket kurtarma planlaması kritik iş süreçlerinin analizini, süreçlerin bağımlı bulunduğu fonksiyonların ve teknolojik alt yapının tespitini, iş süreçlerinin maksimum kesinti dayanma sürelerinin tespitini, hedeflenen kurtarma sürelerinin tespitini, kesinti durumunda uğranılacak zararın boyutuna ve kurtarma zaman hedefine göre gerekli devamlılık ve kurtarma yatırımlarının seçilmesini, etkin bir planlama, eğitim, iletişim ve test döngüsünün uygulanmasını ve kesintiye karşı hazırlıklı kalınmasını, kesinti durumunda kritik süreçlerin kabul edilebilir süre ve seviyede devam ettirilebilmesi için gerekli prosedürlerin hazırlanmasını, kesinti sırasında biriken bilgi ve işlerin bilgi sistemleri ayağa kaldırıldıktan sonra sistem ile senkronizasyonunu, soğuk, ılık veya sıcak kurtarma merkezlerinin oluşturulmasını içerir.

Gizlilik

Ülkemizde henüz bireysel veya diğer kritik bilgilerin gizliliğinin korunmasına yönelik batıdaki nitelik ve çoklukta düzenlemeler bulunmamakla birlikte, bazı ülkelerde birey ile ilişkilendirilebilir sağlık, finansal ve diğer bilgilerin gizlilik içinde saklanması, bu tür bilgilerin aktarımı sırasında güvenlik zincirinin kırılmaması kurumlar için zorunluluktur. Bu nedenle benzer düzenlemelere tabi kurumların kritik bilgilere erişim, kullanım ve bilginin aktarımı sırasında mahremiyet kontrollerini titizlikle uygulaması, kurumun müşteri güveni, itibar ve para kaybetmemesi açısından son derece önemlidir.

Bilgi teknolojileri denetimi

Bilgi teknolojileri denetimi savunma cephelerinin tümünün yukarıdan görülmesi ve savunma gücü hakkında bağımsız güvence sağlanması açılarından son derece önemli bir yönetim fonksiyonudur. BT denetimi kurum içinde bilgi savunma komuta görevini üstlenen yönetim birimine ve kurumun hedeflerine ulaşma başarısı için nihai sorumluluğu taşıyan yönetime son derece önemli bilgiler sağlar.

Bilgi güvenliği yönetimi

Tüm bu savunma yöntemlerinin ötesinde ve öncesinde teknik bir yöntem olmaması nedeniyle teknik personel tarafından itibar görmeyebilecek bir savunma yöntemi vardır ki, aslında tüm savunma çabalarına bu yön verir. Bu yöntem savunma çabalarını yönlendirecek, bilginin korunmasından fayda görecektir ve bilginin korunması konusunda sorumluluk sahibi taraflara yön veren bilgi güvenliği politika, standart ve prosedürleridir. Bilgi güvenliği politikası, savunma çabalarını bir orkestra şefi gibi yönlendirir, bir başka deyişle, savunma kuvvetleri komutanının ortaya koyduğu stratejidir. Standartlar, sürekli bir gelişim içinde olan bilgi teknolojileri alt yapısındaki genişleme ve yeni parçaların alt yapıya eklenmesinin önceden belirlenmiş ve güvenliği onaylanmış olan şekillerde gerçekleştirilmesi için bilgi teknolojileri uzmanlarına yön gösterirler. Prosedürler ise bilgi işleme, erişim haklarının tanımlanması, değiştirilmesi ve kaldırılması, yedeklerin alınması, rutin kontroller ve izleme gibi güvenlikle ilgili tüm operasyonel adımları tanımlar ve her bir operasyonun önceden belirlenmiş biçimde yürümesi için yol gösterir.

BT iletişimi olan iş ortakları, kurum dışından erişim noktaları

Son derece önemli bir savunma alanı da güvenilen dış erişim alanlarıdır. Doğrudan kontrol dışında bulunan bu alanlardaki savunma gücünün yeterliliği hakkında şüphe duymak son derece doğaldır. Bu nedenle, kontrol derecesine bağlı olarak bu alanlara güvenilmez gözle bakmakta ve iletişim noktalarında sıkı kontroller uygulamakta fayda vardır. Bu varsayımın alternatifi, iş ortakları ile yukarıda sayılan diğer cephelerde ortak savunma yapmak veya iş ortağının savunma gücü hakkında bağımsız ve objektif güvence (denetim) sağlamaktır. Kurum dışından gelip de kurum bilgi ağına bağlanması gereken kişilerin, kurum bilgi güvenliği politika ve prosedürlerine uyumu sağlanmalıdır.

Bilgi savunmasındaki temel cepheler yukarıda da belirtildiđi gibi ieride, sınırdaki, sınır dıřında ve hatta bilgi kullanıcılarının zihinlerinde bulunmaktadır. Bu kadar ok cephesi olan bir savunma sisteminin ynetimi ok karmařık olabilir. Bu nedenle yine yukarıda belirtilen bilgi gvenliđi ynetim, kontrol, izleme ve gvence mekanizmaları da son derece nemlidir.

FATİH EMİRAL

Deloitte Kurumsal Risk Hizmetleri

AGUSTOS 2004, ACTIVELINE