

Ađ Güvenlik Denetimine Bakış

Günümüzde dünyamız gözle görülen ve görülmeyen bilgi ađları ile örülmüştür. İletişim yaşamın tüm alanlarında büyük öneme sahip konumdadır. Kurumlar ve kişiler arası iletişim ihtiyaçlarının artması, iletişim ađlarının kurum ve kişilerin varolduđu alanları kapsayacak nitelikte olmasını, dolayısı ile ađlar arası entegrasyonu zorunlu kılmıştır. Kullanıcılara, hizmet sağlayıcılara, müşterilere ve iş ortaklarına her nerede olurlarsa olsunlar bilgi sistemleri imkanlarına erişim imkanı sağlanması gerekmektedir. Böylece neredeyse bütün sistemler birbirleri ile bađlı hale gelmeye başlamıştır.

Bilgi sistemleri arasındaki entegrasyonun bu denli gelişmiş olması bilgi sistemleri güvenliğinde fiziksel güvenlik kontrollerinin kapsayıcılığının azalmasına neden olmaktadır. Şu bir gerçektir ki günümüzde neredeyse her bilgisayar istendiğinde bir diđerine internet vasıtası ile bađlanabilmektedir. Nimda, Code Red ve Lovebug gibi virüs ve kurtçuk programların dünya çapında yayılabilmesi bilgisayarlar arası iletişimin ne kadar yüksek düzeyde olduđunun kanıtıdır. Bu düzeydeki bađlantı gerekli güvenlik tedbirleri alınmadığı takdirde herkese her sistem üzerindeki bilgi ve imkanlara ulaşma yolunu açmaktadır.

Bu konudaki riskler bizi bilgi ađlarının güvenliğinin sağlanması ve denetimi konularında geçerli ve etkin bir yaklaşım ortaya koymaya yönlendirmektedir. Ancak bu aşamada bilgi ađı güvenliğinin genel bilgi sistemleri güvenlik çerçevesinden bağımsız olmadığı ve diđer önemli başlıklar olan uygulama, işletim sistemi ve veritabanı güvenliği, fiziksel ve çevresel güvenlik ve iş sürekliliđi ile birlikte bu çerçevenin bir parçası olduđunu belirtmek gerekir. Yani bilgi sistemleri güvenliğinin en popüler konularından biri bilgi ađı güvenliği olsa da bu konuda güvence sağlamak için bilgi güvenliği kavramını oluşturan tüm parçaların değerlendirilmesi ve denetlenmesi gerekmektedir.

Bir bilgi ađı aynı oda veya bina içindeki birkaç bilgisayarın iletişimine olanak sağlayan küçük bir yerel bilgi ađı olabileceđi gibi, farklı şehirler, hatta ülkelerde bulunan ofis veya fabrikalarda kullanılan bilgi sistemlerini birbirine bađlayan bir geniş alan bilgi ađı olabilir. Bilgi ađları da iş ortakları ve müşterilerin ađlarına, veya internet gibi herkese açık ađlara bađlanabilir.

Bilgi Ađı Risk ve Kontrolleri

Bilgi ađları ile ilişkili temel riskler ve bu risklere ilişkin kontroller 3 ana grup içinde toplanabilir:

İletişimin gizliliđi ve iletişim içeriğinin güvenliği

Bilgi ađları üzerinden iletilen veriler genellikle 3. şahısların fiziksel kontrolünde olan cihaz ve ortamlardan geçer. Verinin üzerinden geçtiđi medyaların izlenmesi, bu medyalara müdahale edilmesi ile verinin gizliliđi ve bütünlüğü tehdit altına girer. Yani veri çalınabilir veya verinin içeriđi deđiştirilebilir, böylece iletişim kuran taraflar iletilen bilginin gizlilik ve bütünlük anlamında kritiklik derecesine bađlı olarak zarara uğrayabilirler.

Sistem odaları, ofisler ve telekomünikasyon hatlarına uygulanan fiziksel erişim kontrolleri, dinleme yolu ile iletişimin izlenmesi tehdidine karşı caydırıcı olacaktır. Bu nedenle bir bilgi teknolojileri denetçisinin ilk değerlendirmesi gereken konulardan biri iletişim hatlarının sonlandığı, bilgi ađı medyalarının geçtiđi ve dağıtımın yapıldığı alanlarda uygulanan fiziksel kontrollerdir. Ancak gelişen teknoloji ve kablosuz iletişimin kullanılması bu kontrollerin etkisini zayıflatmaktadır. İletişimin izlenmesi ve/veya deđiştirilmesine karşı uygulanabilecek en iyi kontrollerden biri bilginin şifrelenmesidir. Eğer şifrelenen bilgiyi ele geçiren kişi deşifre edemiyorsa ele geçirilen bilginin hiç bir anlamı olmayacaktır. Günümüzde pek çok şifreleme yöntemi ve bu yöntemlerin kombinasyon halinde kullanımı söz konusudur. Şifreleme işlemi uygulama yazılımı ile veya donanım ve bilgi ađı cihazları ile iletişim sürecinin farklı noktalarında gerçekleştirilebilir. Sanal özel ađlar (VPN) şifreleme yöntemi ile halka açık ađlar üzerinden sanan bir tünel oluşturarak bilginin gönderilmesine örnektir. Dijital sertifika ve dijital imzalar veri bütünlüğünü ve kimlik tespitini sağlayan

örneklerdir.

Süreklilik

Bilgi ağları geliştikçe ve genişledikçe, daha fazla bilgi sistemleri kullanıcısı uygulama ve verilere uzaktan erişerek hizmet üretmektedir. Bu nedenle bilgi ağı hizmetinin kesintiye uğraması bilgi ağından faydalanılarak yerine getirilen hizmetlerin önemli oranda aksamasına neden olacaktır.

Bilgi ağı hizmetinin sürekliliği ve istenen minimum hizmet seviyesinin sağlanması için en iyi kontrol iyi tasarlanmış bir bilgi ağı mimarisi ve bilgi ağının gözetim altında tutulmasıdır. İyi bir bilgi ağı tasarımı kritik olan her bilgi kaynağı ve erişim noktası arasında yedek kanalları ve bilginin otomatik olarak uygun kanallardan akmasını sağlayacak yönlendirme hizmetini sağlamalı, bu sayede zaman ve veri kaybına yol açmadan iletişimin sürekliliğini garanti altına almaya çalışmalıdır. Bilgi ağını oluşturan tüm bileşenlerin hatalara karşı kendilerini otomatik olarak düzeltme özellikleri olmalı veya uygun bir yedekleme imkanına sahip olmalıdır. Karmaşık ve geniş bilgi ağları gözetim altında tutulmalı ve kolayca yönetilebilmelidir. Bu genellikle bilgi ağı yönetim yazılımları ve 7x24 yardım masası hizmet veren bilgi ağı operasyon merkezleri ile sağlanmaktadır. Bu araçlar kapasite yönetiminin yapılabilmesine, veri aktarımında tıkanma ve kayba uğramadan kullanıcı ve uygulamaların talep ettiği hızda veri iletilmesine de imkan sağlar.

Erişim/Giriş Noktaları

Bilgi ağları, bilgi sistemlerini bir kutu veya odanın ötesine taşımaktadırlar. Bilgi ağları kullanıcıların coğrafi sınırları aşarak bilgi sistemlerine erişimine imkan sağlamış, böylece büyük bir kullanım kolaylığı ve etkinlik artışına yol açmıştır. Ancak bu imkan belli güvenlik zayıflıklarını da beraberinde getirmiş, bilgi sistemlerine pek çok noktadan istenmeyen erişim riskini doğurmuştur. Bilgi ağını oluşturan parçalardan birinde oluşacak kontrol zayıflığı ağ üzerinde bulunan tüm bilgi sistemlerini tehlikelere karşı korunmasız bırakacaktır. Bilgi ağları istenmeyen erişimlere ve kötü niyetle geliştirilmiş yazılımlara pek çok geçiş noktası sağlayabilir. Bu nedenle bilgi ağı giriş noktaları üzerindeki kontroller önem kazanmaktadır.

Bilgi ağı kontrollerinin pek çoğu bilgi ağının dış ağlara bağlandığı noktalarda yoğunlaşmıştır. Bu kontroller bağlantı noktasından akan veri trafiğinin tipini, geliş ve gidiş yönlerini kısıtlar. Örneğin bir kurumun müşteri siparişlerini bildirmeleri için kendi bilgi ağı içinde bulunan web sunucusuna sadece belli tipte trafik (http) ulaşabilmeli bunun dışındaki trafik tipleri (örneğin telnet) engellenmelidir. Bu tür kontroller güvenlik duvarlarının kural setleri veya yönlendiricilerin giriş kontrol listeleri ile uygulanabilir. Anti-virüs yazılımları ve saldırı tespit sistemleri bilgi ağı giriş noktasında kötü niyetli yazılım ve faaliyetleri tespit edebilir ve düzeltici faaliyetleri gerçekleştirebilir.

Kontrol uygulamalarının bilgi ağının diğer ağlara açıldığı noktalarda bulunmasının yanı sıra bir risk analizi ile tespit edilecek kritik sunucular ve bilgi ağının içeride kalan kritik bölümlerinde de yer alması bilgi ağı güvenliğini daha etkin olarak sağlamamıza yardımcı olur. Kritik bilgi kaynaklarının bulunduğu sunucuların işletim sistemlerinin saldırılara dayanıklı hale getirilmesi, uygulama erişim kontrollerinin güçlendirilmesi ve bakımlarının düzenli biçimde yapılması bilgi ağı güvenliğinde yeni katmanlar oluşturacaktır.

Bilgi Ağı Güvenliğinin Denetimi

Bilgi ağı güvenliği denetimini gerçekleştirebilmek için her denetim alanında olduğu gibi denetim alanı, yani ilgili bilgi ağı, hakkında bilgi edinilmelidir. Bilgi ağları hakkında bilgi edinme süreci aşağıdaki adımları izleyerek gerçekleştirilmelidir:

- **Kurumun Bilgi Ağının Kapsamı Nedir?** – İlk adım bilgi ağının kapsadığı alan ve sınırlarının anlaşılmasıdır. Bu genellikle bilgi ağı diyagramı ve dokümantasyonunun incelenmesi ile gerçekleştirilir. Bilgi ağı diyagramı temel olarak bilgi ağının kapsadığı alanları ve iletişim yollarını gösteren bir haritadır. Denetçinin diyagram konusunda dikkat etmesi gereken nokta gerçek durumu yansıttığından emin olunmasıdır. Büyük bilgi ağları iş ihtiyaçlarının karşılanabilmesi için sürekli olarak değişime uğrar. Bu nedenle düzenli olarak güncellenmeyen bilgi ağı diyagramları geçerliliğini kısa sürede yitirir. Bilgi teknolojileri denetçisi, bilgi ağı dokümantasyonunun güncellenmesi için uygulanan prosedür ve kontrolleri anlamalıdır. Diyagramın oluşturulmasında bir bilgi ağı yönetim yazılımı kullanılması diyagramın güvenilirliğini artıracaktır. Hemen her kurumsal bilgi ağında fabrikalar, satış ofisleri gibi çeşitli yerleşimler tarafından ulaşılan, çeşitli sunucuların bulunduğu konsantrasyon merkezleri bulunmaktadır. Küçük bilgi ağlarında bu tür merkezlerden bir tane

bulunurken büyük bilgi ağı üzerinde kritik hizmetlerin sağlandığı birden fazla merkez olabilir. Bilgi ağı diyagramı bilgi ağı üzerindeki cihazlar ve kullanılan protokoller hakkında da bilgi sağlayabilir. Bu nedenlerle bilgi ağı diyagramı denetçiye çalışması boyunca kullanacağı temel bilgileri sağlar.

- **Bilgi Ağı Üzerindeki Kritik Bilgi Varlıkları Nelerdir?** – Bilgi güvenliği sistemi ve bilgi güvenliği denetiminin etkin olabilmesi için geçerli temel prensip, sistematik bir risk analizi sonucunda ortaya çıkan öncelik sırasına göre varlıklara ve ilgili kontrollere odaklanılmasıdır. Denetçinin kritik bilgi kaynakları, sistemleri ve hizmetleri konusunda açık bir fikri olmalıdır. Genellikle uygulama, veritabanı, e-posta, web sunucusu gibi kaynaklar, bu kaynaklara erişim için kullanılan bilgi ağı kaynakları kurumlar için kritik varlıklardır. Bilgi ağı güvenliği kapsamında kritik kaynakların erişim kontrolleri ve işletim sistemi güvenliği yeterli güvence sağlamalıdır.
- **Kimler Erişim Yetkilerine Sahiptir?** – Bir sonraki adım bilgi ağı üzerindeki sistemlere kimlerin erişim hakları olduğunun ve erişimin nasıl gerçekleştirildiğinin ortaya çıkarılmasıdır. Şu soruların yanıtları bilgi ağı güvenliği üzerinde önemli etkiye sahiptir; Bilgi kaynaklarına sadece kurum çalışanları tarafından mı ulaşılmaktadır? Kurum çalışanları ofis dışından da kurumsal bilgi kaynaklarına erişmekte midir? Müşteri ve iş ortakları kurumsal bilgi kaynaklarına erişmekte midir? Müşteri ve iş ortakları sadece internet üzerinden web sunularına mı erişmektedir yoksa kurum bilgi ağına bulunan başka sistemlere de giriş yapmakta mıdır?
- **Kurumsal Bilgi Ağının Dış Dünyaya Açılan Noktaları Nelerdir?** – Bu adım aslında bilgi ağı kapsamının anlaşıldığı ilk adımın bir parçası olmakla birlikte ayrıca ele alınmayı hak eden öneme sahiptir. Günümüzde bilgi ağlarının çoğu en azından internete bağlanmaktadır. İnternet bağlantılarının en temel amaçları e-posta alabilmek ve gönderebilmek, kullanıcılara internet sitelerini kullanma imkanını sunmaktır. Kurumlar elektronik ticaret sitelerini internete açarak, müşterileri ve iş ortakları ile veri alışverişi yaparak ve diğer yöntemlerle kurumsal faaliyet maliyetlerini azaltmak, yeni kanallardan müşterilerine ulaşmak ve iş süreçlerini hızlandırmak için de bilgi ağlarını internet ile buluşturabilirler. İş ortakları ile kurumlar arasında herkese açık olmayan özel hatlar da bulunabilir. Tüm bu bağlantı noktaları dış dünya için potansiyel giriş noktalarıdır. Dış dünyaya bağlantı noktalarının anlaşılması ile denetçi kurumun bilgi ağı sınırlarını tanımış olur. 2. adımın gerçekleştirilmesi ile denetçi zaten hangi bilgi kaynaklarının sadece iç kullanıcılar, hangilerinin hem iç hem de dış kullanıcılar, hangilerinin sadece dış kullanıcılar tarafından kullanıldıklarını biliyor olacaktır. Bu sınıflandırma dışı açık kaynakların yerleştirildiği alan ve bilgi ağı kontrol araçlarının yerleşim tasarımı değerlendirilmesine de imkan tanıyacaktır. Tehditler sadece dış dünyadan yönelmemekle birlikte kontrol kaynaklarının çoğu bilgi ağını dış dünyaya karşı korumak için harcanmaktadır. Ancak kurum içinde bulunabilecek tehditler de en az dışarıda bulunanlar kadar tehlikeli olabilir. Denetçi her iki tarafta bulunan tehditlere karşı uygulanan kontrol mekanizmalarını değerlendirmelidir.
- **Kontrol mekanizmaları nelerdir?** – Bilgi ağı hakkında temel bilgiler, bilgi varlıkları ve riskler anlaşıldıktan sonra denetçi kontrol mekanizmalarını anlamaya, kontrollerin etkinlik ve uygunluklarını değerlendirmeye hazır olacaktır.

Kontrol Mekanizmalarının Değerlendirilmesi

Bilgi ağı kontrol mekanizmalarının değerlendirilmesinde ilk adım dış dünyaya bağlanılan noktalarda yetkisiz erişim ve kötü niyetli yazılımlara karşı alınan önlemlerin değerlendirilmesidir. Bu tehditlere karşı uygulanan kontroller; iyi tasarlanmış bir bilgi ağı mimarisi, uygun iletişim protokolleri ve şifreleme yöntemlerinin kullanımı, bilgi ağı cihazlarının seçim ve konfigürasyonu, güvenlik duvarı, anti-virüs yazılımları ve saldırı tespit sistemi gibi diğer kontrol araçları olarak sayılabilir.

Bilgi ağı kontrollerinin değerlendirilmesi uzman bilgi seviyesini gerektirdiğinden denetim ekibinde, kullanılan iletişim protokolleri, bilgi ağı cihazları ve yazılımlar hakkında uzman bilgi seviyesine sahip denetçiler bulunmalıdır. Bu makalede bilgi ağı denetiminin temel hatları verilmeye çalışılmış olup denetlenen her ortam için gerekli detaylı denetim planlarının düzenlenmesi ve kullanılan araçlar için uzman bilgi seviyesinin edinilmesi gerekmektedir.

Bilgi ağı tehdit ve riskleri oldukça hızlı biçimde artmakta ve değişime uğramaktadır. Benzer biçimde bilgi ağı güvenlik ürünleri de yeni ihtiyaçlara bağlı olarak sürekli değişime uğramaktadır. Bilgi teknolojileri denetçisi bilgi ve deneyim ihtiyacını tespit ettikten sonra gerekli bilginin edinilmesi veya uzman tedarik edilmesi yoluna gidilebilir. Bilgi teknolojileri denetçisinin bilgi ağı güvenlik kontrolleri yönetimi ile ilgili değişim yönetimi ve izleme prosedürlerini anlaması gerekmektedir. Konfigürasyon değişiklikleri, uygun değişim yönetimi prosedürleri izlenerek gerçekleştirilmeli, kontrol noktalarında üretilen log kayıtları incelenmeli ve gerekli önlemler alınmalı, güvenlik ihlallerine karşı izlenecek prosedürler belirlenmelidir. Bilgi ağı güvenliğinin

etkinliđi sadece pahalı ve karmaşıđık araçlar alınması ile sağlanamaz. Bilgi ađı kontrol araç ve prosedürleri düzenli olarak deđerlendirilmeli ve gerekli düzenlemeler gerçekleştirilmelidir.

Fatih Emiral

© 2009 BTRisk. Tüm hakları saklıdır.