

Bilgi Savunmasının Cepheleri

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. Bu varlıklar değer taşıyorsa, elbette profilleri pek çok yerde ifade edilmeye çalışılan kişi ve grupların, çeşitli yöntem ve araçlarla saldırılarına hedef gözeterek veya rastgele uğrayacaktır ve uğramaktadır da. Bu gerçek te toplum genelinin malumudur. Değerli bir varlığa sahip olunduđu ve bu varlığa yönelik tehditler de mevcut olduğunda ihtiyatlı ve mantıklı varlık sahibinin yapması gereken bu varlığı değeri nispetinde savunmasıdır. Yıllık savunma maliyet sınırının ne olması gerektiđi sağlıklı verilerin elde edilebilmesi kaydıyla her bir varlık ve o varlığa yönelik tehdit için aşağıdaki gibi hesaplanabilir:

Savunma Maliyet Sınırı = Yıllık Beklenen Varlık Kayıp Miktarı = Tehdidin Gerçekleşmesi Durumunda Yaşanacak Kayıp Miktarı x Tehdidin Bir Yıl İçinde Gerçekleşme İhtimali

Yani yapılacak savunma yatırımının miktarı beklenen kayıp miktarına eşit veya daha az olmalıdır. Peki bilgi varlıklarımızı hangi cephelerde ve nasıl savunmalıyız? Eğer bilgi varlığımızın 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 yapılsa 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, hatta kağıt üzerine dökülür ve kişilerin belleklerinde yer alır. Sonuç olarak hat ve alan savunmalarını bir arada kullanmak en doğru çözümdür. Çok kritik durumlarda adam adama savunma dahi yapılmalıdır. Önemli olan bu savunma yöntemlerinin ortaya konması ve dengeli biçimde uygulanması, yani savunma yatırımlarının gerekli yerlere ancak dengeli biçimde yapılmasıdır. Bilgi savunmasında kolektif olarak kullanılması gereken bu yöntemler aşağıdaki gibidir;

Güvenlik Organizasyonu;

Bilgi savunmasında bilgiyi bilgi sahibinin isteđi doğrultusunda kullanan ve bilgiden yarar gören herkes bir nefer olmalıdır. Ancak güvenlik organizasyonu daha aktif görevler üstlenmek üzere gereklidir. Böyle bir organizasyonun varlığı bilgiye yönelen tehditlere karşı proaktif önlemler uygulanmasına imkan tanıyacaktır. Bilgi güvenliđi organizasyonu sürekli olarak tehditlerin belirlenmesi, risklerin analiz edilmesi, risklere karşı önlemlerin uygun olanlarının seçilmesi ve uygulanmasından sorumludur. Bu tür organizasyonlara henüz kurumlarımızda sık rastlanmamaktadır. Uygulama geliştirme, sistem, network, veritabanı ve uygulama yöneticilerinden kurumun bütününe gözlemleyecek bir noktada bulunmamalarına rağmen yukarıda belirtilen görevleri yerine getirmeleri beklenmektedir. Böyle bir ortamda gözden kaçan zafiyetlerin doğması, kontrollerin dengeli uygulanamaması, açık ve saldırılara zamanında müdahale edilememesi son derece olasıdır.

Kullanıcı Bilgi Güvenliđi 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 araçlarını ve eriştikleri bilgiyi neden ve nasıl korumaları gerektiđi 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 işbirliğini kazanmayı amaçlamalıdır. Sonuç olarak kurum ortakları, kurumun iş ortakları, bazı durumlarda halk ve ülke, müşteriler ve tabi ki çalışanlar kurum güvenliğinin zarar görmesinden doğrudan veya dolaylı olarak etkileneceklerdir. Bilgi güvenliđi bilinçlendirmesi için eğitim programları hazırlanmalı ve periyodik olarak tekrarlanmalıdır. Bilgi

sahiplerinin doğrudan ve kesin olarak kontrol edemeyeceği en önemli nokta kullanıcılarıdır. Bu nedenle kullanıcıların ikna edilebilmesi için güçlü kanıtlar, hazırlık ve sabır gereklidir.

Bilgi Teknolojileri Çözümleri Üretenlerin Bilgi Güvenliği Bilinci;

Güvenlik sistemlerinin maliyeti mevcut bilgi sistemlerine sonradan eklenme 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 imkan sağlamalıdır. Bilgi sistemlerinin bilgi güvenliği bilinci ile tasarlanması ve üretilmesi kurumu daha sonra oluşacak risk ve maliyetlerden koruyacaktır.

Kimlik Yönetimi;

Bilginin saklandığı ortam ve bilgiye iletişim platformlarının artması çok sayıda kullanıcı bilgisinin saklanmasını, dolayısı ile kullanıcılar tarafından çok sayıda kullanıcı kodu ve şifrenin hatırlanmasını zorunlu kılmıştır. Farklı ve çok sayıda giriş kontrol noktasının olması, kullanıcıların kolay şifre seçmesi, şifrelerini yazması, farklı platformlarda farklı şifre kriterlerinin uygulanması, işe başlayan, görevi değişen, işten ayrılan personel için operasyon yükünün artması veya ihmali ihtimalinin artmasına neden olmaktadır. Bu sorunu bertaraf etmek için kimlik yönetimini tek noktaya toplayan standartlar ve araçlar geliştirilmiştir. Yukarıda sayılan sorunları ortadan kaldırmaya yönelik bu çözümler kullanıcı şifresinin ele geçirilmesi durumunda birden fazla kaynağa erişim sağlayabileceğinden kuvvetli şifre kriterlerinin kullanılması ve kullanıcı bilinci büyük öneme sahiptir.

Uygulama Güvenliği ve Bütünlüğü;

Uygulamalar ve diğer raporlama araçları bilgi üretim ve kullanımı için en önemli araçlardır. Bu araçlar iş süreçlerine uygun olarak tasarlanmakta, farklı kullanıcı profilleri için farklı ihtiyaçları yerine getiren modülleri barındırmaktadırlar. Uygulamalar altyapı 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 kayıtlarını yeterince veya hiç tutmamaları, 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 altyapılarındaki açıkların sadece teknik olması gerekmez. Kullanıcı hakları tanımlama konusundaki prosedürel eksiklikler veya kurum iş süreçlerinde rollerin ayrımı ilkelerinin uygulanmaması kurumun uygulamalar aracılığı ile zarara uğratılmasına imkan tanıyabilir. İnternet uygulamaları, kurum bilgi kaynaklarına açılan kapıyı daha geniş kitlelere ulaştırdıklarından bu uygulamaların çalıştığı platformlara özgü ve genel uygulama zafiyetlerini özellikle dikkat edilmeli ve gerekli kontroller uygulanmalıdır. Tüm uygulama geliştirme personelinin çalıştığı platformlar ile ilgili güvenlik konularında bilgi sahibi olması gerekmekte, ancak internet 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. Bilgi de üretilir, üretilmesi için kaynak harcanır ve sonunda müşterileri tarafından kullanılır. Dolayısı ile bilgi de bir kalite maliyetine sahiptir. Bilginin oluşmasını sağlayan veriler kurumlar tarafından yeterli veya yetersiz üretilir, iyi veya kötü organize edilmiş depolarda saklanır ve verimli veya verimsiz biçimde veriden bilgi üretmek üzere faydalanılır. Bu süreçlerde uzun vadede kalitenin maliyet artışına neden olmadan yükseltilmesi mümkündür. 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 düzenleme ile kullanılan veritabanı yönetim sistemleri saldırılara açıktır. Aynı zamanda tüm sistem yazılımları gibi keşfedilmiş veya keşfedilmeyi bekleyen açıkları barındırmaktadırlar. Bilginin büyük zamanını geçirdiği ve

toplucu ulařılabildiđi bu ortamların korunması son derece önemlidir. Veritabanı gvenliđinde en kritik nlemlerden biri veriye sadece uygulamalar aracılıđı ile eriřime izin verilmesidir. Tm uygulamalar iin olduđu gibi hem BT personeli hem de son kullanıcılar iin veritabanına dođrudan ulařan uygulamaların (utility'ler) kurulumları BT ve gvenlik ynetiminin kontrolnde sadece ihtiya olması durumunda yapılmalıdır. Veritabanı profilleri iin kullanılan Őifreler kaba tahmin yntemlerine dayanıklı karmařıklık ve uzunlukta olmalı, dzenli veri yedekleri alınmalıdır. Veritabanı sistemlerine bilgi ađı zerinden eriřim mmkn olduđunca denetlenmeli, veritabanına yapılan eriřimler en azından yksek yetkili kullanıcılar iin incelenmek zere kaydedilmelidir.

İletişim Gvenliđi;

İletişim giriř noktaları fiziksel savunma hattından sonraki (veya nceki) ilk savunma hattıdır. İletişim gvenliđi iletişim kanalının ulařtıđı bilginin kritikliđine gre kurum dıřı iin olduđu gibi kurum ii iin de gerekli olabilir. Gnmzde kablosuz iletişim teknolojisi de kullanılmaya bařlandıđından fiziksel sınırlar nemini yitirebilmektedir. İletişim dnyası kendine has protokollerle ve kanallar zerinden alıřmaktadır. Bu protokoller ođunlukla standart olup herkes tarafından bilinmektedir. Kurumlar kendi kontrolleri altında olan ve olmayan kanallar zerinden bilgi alıř veriři gerekleřtirmektedirler. İletişim kanalları tm uzaktan saldırılar iin kullanıldıđından ok eřitli saldırı tiplerine karřı korunmalıdırlar. İletişim gvenliđinde gizlilik, btnlk ve eriřilebilirlik kriterlerinin hepsi geerlidir. Gizlilik ve btnlk iin Őifreleme zmleri, ve sınır noktalarında sadece ihtiya duyulan protokoller iin ve mmknse istenen noktalardan gelen giriř ve ıkıř taleplerine izin verilmelidir. Eriřilebilirliđe ynelik ve diđer tehditlerin hızlı algılanabilmesi iin kritik sunucular zerinde veya iletişim hatları zerinden gelen, akan iletişim paketlerini dinleyen saldırı tespit sistemleri kullanılmalıdır. İletişim gvenliđinde kullanılan giriř kontrol aralarının belirlenmiř aıkları kapanmıř gncel versiyonlarının kullanılması hayati nem tařımaktadır. İletişim mimarisinin bilgi kaynaklarının niteliklerine uygun olarak dzenlenmesi, dıřarıdan gelen paketlerin kurum iine dođrudan alınmaması nemli bir maliyet farkına neden olmayan ancak bilgi gvenliđine byk katkısı olan bir uygulamadır. İerideki bilgi kaynaklarının bulunduđu platformlara iliřkin dıřarıya bilgi sızdırılmaması iin gerekli kontrollerin uygulanması, dıřarıya bilgi veren servislerin kapatılması da muhtemel saldırılar iin saldırganların ihtiya duyacakları bilgiye ulařmalarını zorlařtıracaktır.

Zayıflık Denetimi;

Kurumlar bilgi sistemleri altyapılarında eřitli retici firmalar tarafından retilmiř sistem ve bilgi ađı yazılımlarını kullanmak zorundadırlar. Bu yazılımlar uygulamalar ve veri kaynaklarının altyapılarını sađladıklarından bu sistemlere giriř bilgiye aılan kapı olabilir. Sistem yazılımları tm dnyada kullanıldıđından bu sistemlerin aıklarını keřfetmek iin uđrařan pek ok kiři bulunmaktadır. Bu kiřiler iyi veya kt niyetlerle buldukları aıkları internet zerinden tm dnya ile paylařmaktadır. Yaklařık olarak gnde 20 sistem aıđının internet zerinden aıklandıđı tahmin edilmektedir. Bilgi teknolojileri saldırılarının ok nemli blm aıklanmıř ve bilinen zayıflıklar kullanılarak gerekleřtirilmektedir. Bu nedenle kurumların bilgi sistemlerini saldırganlardan korumak iin kullanmakta oldukları sistemler ile ilgili aıkları yakından takip etmeleri, retici firmalar tarafından geliřtirilen zmleri bir an nce uygulamaları ok nemlidir. Sistem yazılımlarında son versiyonların takibi zellikle dıř dnyaya aılan veya kritik bilgi kaynaklarını barındıran sistemler iin bir zorunluluk haline gelmiřtir. Bir bařka aktif savunma yntemi de kurum sistemlerinin periyodik olarak zayıflıklara karřı taranmasıdır. Bu sayede hem bilinen aıklar hızlı biimde tespit edilmiř olur, hem de son denetimden sonra standartlar ile uyumsuz veya yetersiz gvenlik ayarları ile kurulmuř sistemler tespit edilebilir. Bu denetimler kurum i ve dıř bilgi ađından yapılabilir.

Virs Koruması;

Virs uygulamaları bařka uygulamalara kendilerini ekleyerek bu uygulamalar aracılıđı ile veya dođrudan kendilerini bilgi ađı zerindeki diđer sistemlere kopyalayarak ođalırlar. Bu nedenle hem bilgi ađı hem de dosya dolařımı (zellikle e-postalar aracılıđı ile) kontrol edilmelidir. eřitli platformlar iin geliřtirilmiř anti-virs yazılımları bulunmaktadır. En etkili yaklařım tm bilgisayarlarda anti-virs yazılımlarının bulunması, virs imzalarının gncellenmesi, bilgi ađı giriř noktasında, e-posta sunucusu zerinde ve kiřisel bilgisayarlar zerinde uygun modllerinin bulunması, anti-virs uygulamalarının dosya kopyalama ve alıřtırma sırasında virs kontrol yapması, virs tespiti zerine sistem yneticisinin uyaracak biimde ayarlanmıř olması, BT ynetimi tarafından onay verilmeyen uygulamaların kurulumuna izin verilmemesi, uygulama kurulumunun BT kontrolnde olması, "worm" saldırılarını tespit etmek iin saldırı tespit ve koruma duvarı kullanılması, virs tespiti durumunda virs bulařmıř sistemlerin bilgi ađından izole edilmesi iin gerekli prosedrlerin oluřturulması, mmknse farklı katmanlarda farklı firmaların rettiđi anti-virs yazılımlarının kullanılmasıdır. Diz st bilgisayar kullanıcıları ve kurum dıřından internete veya bařka

kurum bilgi ađlarına bađlanan kullanıcılar virüs güvenliđi konusunda bilinçli olmalı ve anti-virüs yazılımlarının virüs imzalarını güncellemelidirler. Bilgi savunmasının tüm cephelerinde olduđu gibi tüm önlemler alınsa dahi bilginin doğası geređi bazı açıklar olabileceđi ve virüs bulaşma riskinin olduđu ancak alınacak önlemlerle en aza indirgeneceđi unutulmamalıdır.

Günlük Tutma, İzleme ve Raporlama;

Bilgi sistemlerine yönelik saldırılar genellikle kullanılan sistemlerin zayıflıklarından faydalanmak amacı ile sistemlerin tespit edilmesini gerektirir. Bilgi sistemleri kutudan çıkmış halleri ve güçlendirilmiş ayarları ile kendilerine yapılan talepleri, üzerlerinde gerçekleştirilen işlemleri kaydedebilir. Bilgi güvenliğine yönelik hazırlanmış 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 kaynađı ve disk kaybından başka bir işe yaramazlar.

Fiziksel Güvenlik;

Medeniyetimiz ne kadar gelişmiş olsun tüm tehditler karmaşık ve bilgi ađları 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 dinlenerek 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 ve statik elektriđe karşı yeterli önlemlerin alındıđı ortamlarda saklanması sayılabilir.

İş Sürekliliđi ve Felaket Kurtarma;

Fiziksel güvenlikle yakından ilgisi bulunan bu alan kesintilere karşı iş süreçleri ve teknik altyapı konusunda yapılacak hazırlık, eğitim ve testleri kapsar. Özellikle büyük ve karmaşık iş süreçlerine sahip kurumların bilgi teknolojileri bađımlılıđı artmış, bu durum BT hizmetlerinin kesintisini daha kritik öneme kavuşturmuştur. İş sürekliliđi ve felaket kurtarma kritik iş süreçlerinin analizini, süreçlerin bađımlı bulunduğu fonksiyonların ve teknolojik altyapının tespitini, maksimum kesinti dayanma süresinin tespiti, hedeflenen kurtarma süresinin tespiti, 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 ayađa kaldırıldıktan sonra sistem ile senkronizasyonunu, sođuk, ılık veya sıcak kurtarma merkezlerinin oluşturulmasını içerir. Bilgi teknolojileri veya başka bir fonksiyonun hizmetinin kesintiye uğraması kuruma para ve itibar kaybettirebilir. Belli bir süreden sonra kurum faaliyetlerine hiç devam edemeyecek hale gelebilir.

Gizlilik;

Ülkemizde henüz bireysel bilgiye yönelik düzenlemeler bulunmamakla birlikte, bazı ülkelerde birey ile ilişkilendirilebilir sađlık, finansal ve diđer bilgilerin gizlilik içinde saklanması, bu tür bilgilerin aktarımı sırasında güvenlik zincirinin kırılmaması kurumlar için zorunluluktur. Bu sorumluluđu yerine getirmemenin, hem gelişen toplum bilinci hem de düzenlemeler nedeniyle kurumlar için önemli sonuçları doğabilmektedir.

Bilgi Teknolojileri Denetimi;

Bilgi teknolojileri denetimi savunma cephelerinin tümünün yukarıdan görölmesi ve savunma gücü hakkında bađımsız güvence sađlanması açılarından son derece önemli bir yönetim fonksiyonudur. BT denetimi bilgi savunma komutanı ve kurumun hedeflerine ulaşma başarısı için nihai sorumluluđu taşıyan yönetime son derece önemli bilgiler sağlar. Bilgi teknolojileri denetimi iç veya dış denetim ekipleri tarafından yapılabilir. Ancak karmaşık sistemler için iç denetim organizasyonunun BT denetim yeteneđinin bulunması, gerekli durumlarda veya uzmanlık gereken konularda dış destek kullanılması en etkili yöntem olacaktır. Elbette tüm alanlar için olduđu gibi bu konudaki maliyetler sađlanacak fayda ile doğrudan ilişkilili olmalıdır.

Bilgi Güvenliđi 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 görecek ve bilginin korunması konusunda sorumluluk sahibi taraflara yön veren bilgi güvenliđi politika, standart ve prosedürleridir. Bilgi güvenliđi politikası savunma çabalarını bir orkestra şefi gibi yönlendirir, bir başka deyişle savunma kuvvetleri komutanının ifadeleridir. Standartlar sürekli bir gelişim içinde olan bilgi teknolojileri altyapısında önceden belirlenmiş ve güvenliđi onaylanmış olan şekillerde genişleme ve yeni parçaların altyapıya eklenmesine imkan tanır. Prosedürler ise bilgi işleme, erişim haklarının tanımlanması, deđiştirilmesi 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. Ortaya konan politika, standart ve prosedürlere uyum ilgili yöneticilerin sorumluluğunda olup denetim fonksiyonu tarafından üst yönetime belirlenmiş kurallara uyum konusunda güvence sağlanır.

ve BT İletişimi Olan İş Ortakları, Kurum Dışından Erişim Noktaları

Son derece önemli bir savunma alanı da güvenilen dış erişim alanlarıdır. Doğrudan kontrol dışında bulunan bu alanlardaki savunma doğal olarak şüphe uyandıracaktır. Bu nedenle kontrol derecesine bađlı olarak bu alanlara güvenilmez gözle bakmakta fayda vardır. Bu varsayımın alternatifi iş ortakları ile yukarıda sayılan diğer cephelerde ortak savunma yapmak veya iş ortağının savunma gücü hakkında bađımsız güvence (denetim) sağlamaktır.

Bilgi savunmasındaki temel cepheler yukarıda da belirtildiđi gibi içeride, bilgi kullanıcılarının zihinlerinde, sınırdaki ve hatta sınır dışında bulunmaktadır. Bu kadar çok cephesi olabilen bir savunma sisteminin yönetimi çok karmaşık olabilir, bu nedenle yine yukarıda belirtilen kontrol, izleme ve güvence mekanizmaları da son derece önemlidir.

Fatih Emiral