Türk Arşivciler Derneği

Arşiv Dünyası Dergisi

The Journal of Archival World

Sayı/Number: 17-18, Sayfa/Pages: 1-10
İstanbul, İlkbahar-Kış/Spring-Winter 2017

ISSN: 2147-2599

KURUMSAL HAFIZANIN KORUNMASINDA SİSTEMİN ÖNEMİ*

The Importance of the System in Maintaining Organizational Memory

Erkan ÖZHAN
Namık Kemal Üniversitesi, Çorlu Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü.
erkanozhan@gmail.com

Alındığı tarih: 15.02.2017; Kabul tarihi: 18.08.2017

Öz

Bu çalışmada kurumsal hafızanın korunmasında sistemin önemi anlatılmaya çalışılmıştır. Günümüzde özellikle elektronik ortamda tutulan kurumsal bilgilerin miktarı devasa boyutlara ulaşmıştır. Kurumlar, bilgi ve belge yönetiminde kullanılan donanım ve yazılım temelli sistemleri sıklıkla kullanmakta hatta bunlar kurumların hayati parçası haline gelmektedir. Bilgi kurumlar için önemli bir servettir. Kurum içerisinde geçmişten gelen bilgi havuzu -ki kurumsal hafıza olarak ta isimlendirilir, belirli bir sistematiği ve esnekliği olan koruma sistemleri tarafından yönetilmelidir. Uygun olmayan koruma, depolama sistemleri, bilginin normal kullanılmasını zorlaştırabileceği gibi, yetkisiz erişimlere, kullanımlara, bilginin bozulmasına vb. neden olabilir. Bu çalışmanın birinci kısmında kurumsal hafızayı oluşturan ana unsurlar, ikinci kısmında dijital koruma sistemlerinin önemi ve bu sistemlerin çalışma prensipleri, üçüncü kısmında koruma sistemini tehdit eden unsurlar ve son bölümde ise çözüm önerileri yer almıştır.

Anahtar Kelimeler: Kurumsal hafıza, güvenlik, savunma, güvenlik sistemleri.

* Bu makale 17/11/2016 tarihinde XI. Türk Arşivciler Günü sempozyumunda sunulan bildirinin geliştirilmiş ve göden geçirilmiş halidir.

Abstract

In this study it is intended to indicate how important security systems are in protecting organizational memory. Today, the amount of institutional knowledge which is stored especially in electronic environment has become massive. Institutions use hardware- and software-based systems which are used in knowledge and document management more frequently and, moreover, these systems prove a vital part of institutions. In other words, knowledge means a fortune for them. The repository of knowledge, coming from the past, also called organization memory, should be managed using the security systems which are systematic and flexible at a certain level. Inappropriate security and storage systems may make the normal use of knowledge difficult and also they may lead to unauthorized access and use, knowledge distortion, etc. The first part of the study deals with the main components forming organizational memory and the second one deals with the importance of digital security systems and their working principles. As for the third chapter, it discusses threats to security systems. In the final chapter, solutions to these threats are recommended.

Keywords: Organizational memory, security, defense, security systems.

Giriş

20. Yüzyılda kilit teknoloji veri toplama, işleme ve dağıtım oldu (Tanenbaum ve Wetherall, 2011, s. 1). Günümüzde ise bilgiye erişmek ve toplamaktan çok bu veriler içerisinden anlamlı bilgiyi tespit etmek, veriler arasında gözle görülmeyen ilişkileri yakalamak ve güvenliğini sağlamak önemli hale gelmiştir. Özellikle elektronik sistemler, bilgisayar yazılımları ve internet her gün milyarlarca bilgiyi insanoğluna ulaştırmaktadır. Kamu ve özel kuruluşlar bilgi deposu haline dönüşmüştür. Bilgiye her yerden ulaşılabilir olması bilginin yayılmasını kolaylaştırmakla birlikte özel bilgi taşıyan dijital belgeler için güvenlik riski de artmıştır. Bilginin yayılması ve bilgi talebinin artışı ile bilgi birçok kurum için sermaye ve kazançla eşdeğer hale gelmiştir. Tüm bu gelişmeler sonucunda, dijital belgeler halinde medya[1] ortamlarına taşınmış olan her türlü resim, yazı, ses, görüntü vb. türdeki bilgilerin güvenliğinin sağlanması gerekli ve başlı başına yürütülmesi gereken ayrı bir iş haline gelmiştir.

Dijital belgelerin yönetimi; devletler, işletmeler, üniversiteler ve hatta kişiler için oldukça önemlidir. Bu belgelerin oluşturulması, depolanması, dağıtımı, silinmesi olmak üzere tüm belgelerin yaşam döngüsünün güvenli ve kolay erişilebilir olması sağlanmalıdır (Zhao, Hu, Li ve Du, 2009, s. 995).

Bilgi sistemlerindeki verinin güvenliği en önemli hedeflerden biridir, bu aynı zamanda bilginin bütünlüğü, gizliliği ve erişilebilirliği ile doğrudan ilgilidir (Stallings, 2011, s. 3).

Günümüz teknolojisi devasa büyüklükte veriyi saklama yeteneğine sahip fakat eğer elimizdeki iş ile alakalı bir bilgiyi bu veriler içerisinden araştırıp bulamıyorsak bu veri faydasızdır (Munier, 2011, s. 16) ve bir bakıma veri kaybı demektir. Benzer

[1] Medya: Bilgisayar biliminde verilerin depolandığı dijital ortamların genel adı.

şekilde depolanmış verilerin güvenliğini sağlayan sistemlerin olmaması da çok ciddi veri kayıplarına neden olabilir.

Günümüzde verileri her yerden ulaşılır kılma çabası ağırlığını güvenliğe göre daha çok hissettirmektedir. Bu nedenledir ki veriler paylaşıma açıldıktan veya kullanıma sunulduktan sonra güvenlikleri ile ilgili önemler alınmaya başlanmakta kısacası güvenlik ikinci aşamada değerlendirilmektedir. Bu ciddi ve hayati bir hatadır. Çünkü veri birçok işlemin ana kaynağıdır, anahtarıdır. Bu anahtarın yetkisiz kişilerin eline geçmesi, istenmeyen birçok durumun zincirleme biçimde ortaya çıkmasına neden olabilir.

Dijital güvenlik sistemleri günümüz bilgisayar sistemlerinin temelinde bulunan parçalardan biridir. Bu sistemler doğru ve kurum gerekliliklerini karşılayacak şekilde yapılandırıldığında koruma görevini başarıyla yerine getirecektir. Ancak bu sistemlerin de gelişen ve değişen veri yapılarına ve iletişim tekniklerine göre yeniden güncellenmesi gerektiği unutulmamalıdır.

Kurumsal hafızaya dokunan ve onun üzerinde birçok değişimin oluşmasına neden olan bir diğer unsur ise personeldir. Personel, güvenlik açısından en kırılgan noktalardan biridir. Çünkü güvenlik sistemleri için istisnai durumlar, unutma, hata yapma doğru programlandığı sürece mümkün değildir. Ancak insan bu manada sayılan olumsuzlukları gerçekleştirebilir. Bu açıdan tek başına güvenliği sağlamada güvenlik sistemlerinin yanı sıra personelin de bu sistemleri destekler şekilde davranması gereklidir.

2. Kurumsal Hafıza ve Ana Unsurları

Hafıza/bellek terimi, algı ya da deneyimlerin gerçek zaman diliminden daha uzun süre saklanmasını ve onlara daha sonra ulaşılmasını mümkün kılan yapı-sistem olarak tanımlanmaktadır (Brookshear ve Brylow, 2002, s. 83) ve gönderen ile alıcı arasındaki bağlantıdan bağımsız kalıcı kayıttır (Lehner ve Maier, 1998, s. 2).

Kurumsal hafızanın tanımlanmasında önemli farklılıklar vardır çünkü kavram, başlangıçta sosyoloji biliminden ödünç alınmış ve daha sonra çeşitli şekillerde yeniden yorumlanmıştır. E.W. Stein'e göre (1995, s. 7) kurumsal hafıza, kurumsal hafızanın içeriği ve kurumsal hafızaya ilişkin süreçler olarak tanımlanır. Yazarın tanımı içerisinde geçen kurumsal hafızanın içeriği incelendiğinde özünde kurumların;

- Bilgi sistemleri,
- Yönetim,
- Ekonomi,
- Sistem,
- Karar verme ve iletişim,
- Kurumsal strateji,
- Kurumsal eserler, üretim vb.

teorileri ve faaliyetleri hakkındaki tüm bilgilerin ve kayıtların olduğu görülür. Bunlar son derece değerli ve geleceğe miras bırakılması büyük kazanç sağlayacak unsurlardır. Bu yüzden koruma stratejilerinin ve alt yapılarının özenle kurulması ve işletilmesi gerekir.

Bilgi yönetimi ise bu bağlamda yine önemli unsurlardan biridir. Bilgi yönetiminin hedefleri, kurumda bilginin büyümesini, iletilmesini ve muhafazasını sağlamaktır (Dieng, Corby, Giboin, & Ribière, 1999, s. 567).

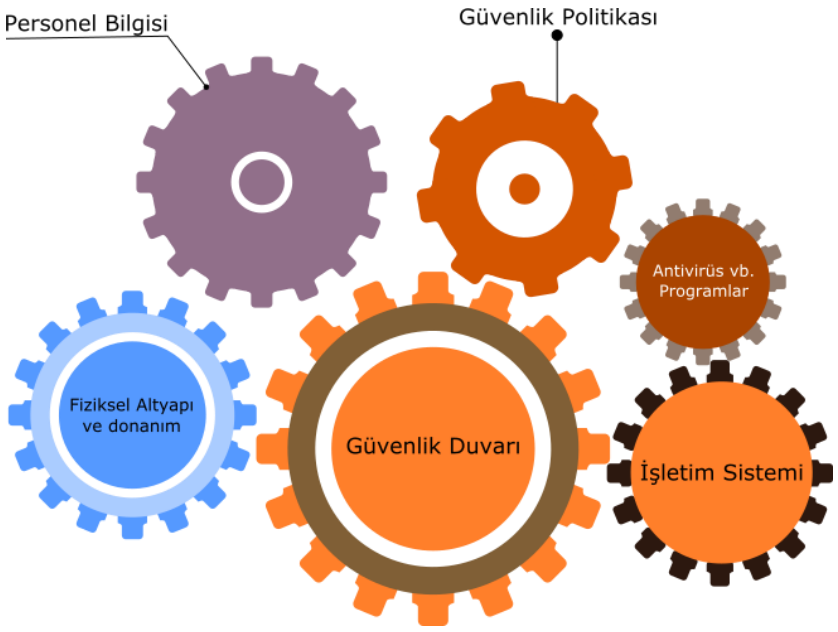
Günümüzde kurumsal hafızanın büyük bölümünü dijital belgeler oluşturmaktadır ve sayıları gittikçe artacaktır. Bu nedenle bu çalışmada kurumsal hafızada önemli bir paya sahip dijital hafızanın korunması konusu ele alınmaktadır. Kurumlar içerisinde dijital bilgi; 1) dosyalar (metin, resim, video, ses ve program kodları) ve 2) veri tabanları şeklinde saklanmaktadır. Bu verilerin bazıları basılı belgelerin dijital halidir. Bazıları ise aynı şekilde dijital bilginin fiziksel basılı hali olabilir. Her ne şekilde olursa olsun bilgi değerlidir ve korunması gerekir.

3. Dijital Hafıza Koruma Sistemleri

Bilgi, şirketleri, kurumları birbirinden ayıran ve diğerinden daha başarılı hale getiren yardımcı kaldıraç görevi görür (Rhodes-Ousley, 2013, s. 3) Koruma sistemlerinin ne kadar önemli olduğu bu kazanımların kaybı ile kendiliğinden ortaya çıkacaktır. Bilginin güvenliği denildiğinde sadece yetkisiz kişilerin eline geçmemesi anlaşılmamalıdır. Dijital bilgi güvenliği, elektronik ortamda dolaşan veya kaydedilmiş bilgilerin korunması ile ilgilenir.

Koruma sistemlerinin tamamında ana amaç, bilginin gizliliğini (confidentality), bütünlüğünü (integrity) ve kullanılabilirliğini (availability) sağlamaktır.

Koruma sistemlerinin yapısına bakıldığında ise Şekil.1'de görüldüğü gibi birbirine bağlı birçok bileşen dikkat çekmektedir. Bu bileşenlerden birinin görevini yerine getirmemesi veya eksik kalması güvenlik açığını doğurabilir.



Şekil 1: Koruma sistemi mimarisi

Sistemi oluşturan bileşenlerin her biri uyumlu ve hatasız çalışırsa sistemin güvenliği maksimum seviyeye ulaşmış olur. Sistemde meydana gelecek herhangi bir

eksiklik ise güvenlik açığına neden olabilir. Şekil.1'de gösterilen sistem mimarisi kurumlar için yapısal açıdan farklılık gösterebilir. Çünkü her kurumun ihtiyaçları farklıdır ve dolayısıyla sistemden beklentileri farklı olduğu için ana yapı değişmese de ayrıntılarda değişiklikler olacaktır.

3.1 Güvenlik Duvarı (Firewalls)

Güvenlik duvarı (GD), kurumsal koruma sisteminin temelini ve kalbini oluşturur. Özellikle çoğu kurumsal ağın internete sürekli bağlı olduğu günümüzde dış dünyadan kurum içine gelen bağlantıları ilk olarak güvenlik duvarları karşılar. Bunun yanında GD, kurum içinden dışarıya doğru yönelen bağlantıları da üzerinden geçirir. Bu özelliklerinden dolayı GD, kurumun ihtiyaçlarını giderecek şekilde doğru ve yeterli bir şekilde yapılandırılmalıdır.

Güvenlik duvarları özel donanımlar üzerinde çalışan yazılımlardır. Yazılım içerisinde yer alan konfigürasyon (yapılandırma) ara yüzü sayesinde kurumun sistem yöneticisi gerekli ayarlamaları yapar. Ancak bunu yapmadan önce kurumun ihtiyaç ve beklentilerinin çok iyi analiz edilmiş olması gerekir. Sonradan ortaya çıkabilecek yeni güvenlik tehditlerine karşı bu konfigürasyonlar güncellenebilir olduklarından bu işlem sistem yöneticisi tarafından gerçekleştirilmelidir.

Güvenlik duvarları, ağ sisteminde güvenlik tehditlerine karşı yerel bir sistemi veya ağ sisteminin genelini korumanın etkili aracıyken, aynı zamanda geniş alan ağları(WAN-World Area Network) üzerinden internete-dış dünyaya erişim sağlıyor olabilir (Stallings, 2012, s. 146).

Güvenlik duvarları kurumsal sistemlerin ve dolayısı ile barındırdıkları hafıza gibi önemli unsurların korunmasında en önemli gerekliliklerden biridir. Günümüzde yapay zekâ tabanlı güvenlik duvarlarının geliştirilmesi ile bu unsur daha da güç kazanmıştır.

3.2 Güvenlik Politikası

Güvenlik politikası; kimlerin veya nelerin belirli bir sistem kaynağına erişebileceğini ve neler yapmaya yetkili olduğunu (Stallings, 2012, s. 146) belirten önceden tanımlanmış ve kararı alınmış güvenliğin işleyiş düzeni ve kapsamının belirlendiği kurallar ve yönergelerdir. Güvenlik politikası sistemin güvenliğini sağlamak için neye izin verilip verilmediğini detaylı olarak açıklayan tanımlardır (Bishop, 2003, s. 67). Sistem izin verilmeyen bir durumu gerçekleştiriyorsa güvensizdir.

Kurumların bilişim sistemlerini kurarlarken bu konuyu birinci öncelikli alan olarak belirleyip güvenlik tutum ve anlayışını yazılı olarak tespit ederek bu çerçevede güvenlik alt ve üst yapısını hazırlamaları çok önemlidir. Ancak günümüzde bu konu en sona bırakılarak ihmal edilmekte ve bir güvenlik ihlali söz konusu olduğunda gerçekleştirilmeye çalışılmaktadır.

Her kurum için geçerli bir güvenlik politikası belirlemek, kurumların güvenlik düzeyleri ve bunu sağlamaya yönelik ihtiyaçları farklı olduğundan teorik olarak mümkün olmamaktadır. Bu nedenle kurumlar kendilerine özel güvenlik politikasını üretmeli ve hayata geçirmelidir.

3.3 Personel Bilgisi

Kurumların bilgiyi toplayan, ona dokunan ve şekil veren yegâne unsurları sistemi kullanan kullanıcılardır. Bu nedenle kullanıcıların kurumsal hafızayı korumdaki rolü üst seviyedir. Kullanıcıların bilgi üzerinde gerçekleştireceği işlemler başta olmak üzere sistem güvenliği ile ilgili eğitim almaları ve aldıkları eğitimi uygulayıp uygulamadıklarının kontrolü kurumsal hafızanın korunması açısından önem arz etmektedir.

Sistem kullanıcıları belirli aralıklarla güncel tehdit unsurlar ve bilgi kaçağına neden olabilecek saldırılara karşı bilgilendirilmelidir.

3.4 Antivirüs vb. Programlar

Şimdiye kadar bahsedilen kurumsal hafıza koruma sistemi unsurları tek başına güvenliği sağlama hususunda yeterli değildir. Güvenliğin bir ağaç yapısı gibi olduğu düşünülürse her bir unsurun kendine göre bir açığı eksiği kapattığı söylenebilir. Bunlardan biri de anti virüs programlarıdır.

Virüs, programlara dilleri ile yazılmış, bulaştığı bilgisayarda çoğalarak sistem kaynaklarını veya verileri tahrip etmeyi amaçlayan zararlı programlardır. Çoğu virüs çalıştırıldığında kendisini diğer programlara ve bilgisayarlara bulaştırır. Bununla birlikte bazı virüsler işletim sisteminin bazı bölümlerini parçalamak, diğer programları bozmak gibi yıkıcı eylemleri gerçekleştirebilirler (Brookshear ve Brylow, 2014, s. 192).

Virüslerden başka, worms, bots, keylogger gibi kurumsal sistem güvenliğini tehdit edici birçok benzer program tehdit unsuru olabilir. Bu ve benzeri tehditleri ortadan kaldırmak için genel adı “Anti Virüs” programı olan ancak benzer zararlı unsurları da tespit ederek engelleme ve silme işlemini gerçekleştiren yazılımlar mevcuttur. Kurumsal hafızanın korunmasında bahsi geçen her unsur son derece önemli olması yanında anti virüs yazılımlarının kurumsal ağa bağlı tüm aygıtlarda kullanılması da önemli bir önleme aracıdır.

3.5 İşletim Sistemi

İşletim sistemi, bir bilgisayarın genel işletimini kontrol eden yazılımdır. Kullanıcının dosyaları saklaması ve erişebilmesi için gerekli ara yüzleri, programları yükleyebilmek ve yürütmek için de gerekli ortamı sağlar (Brookshear ve Brylow, 2014, s. 127). Kurumsal hafızayı oluşturan sistemler büyük oranda işletim sistemi üzerine inşa edilir. İşletim sisteminin güvenlik açıklarının olması sistemin de açık vermesine neden olabilir. Güvenlik açısından tasarımı iyi bir işletim sistemi aynı şekilde güvenliği sağlamlaştırıcı katkı sağlayacaktır. Bunun yanında işletim sistemi kullanıcıların görev performanslarını artırıcı özellikler de içermelidir. Günümüzde çok sayıda olmasa da birçok kurumsal hafıza sisteminin ihtiyaçlarını karşılayacak düzeyde geliştirilmiş işletim sistemi seçeneği mevcuttur. İşletim sistemini iki şekilde düşünmek mantıklı olur. İlk olarak ana bilgisayar dediğimiz bilgisayar üzerinde çalışacak olan işletim sistemi ve ikinci olarak kullanıcıların işlemlerini yapmaları için sunulmuş olan istemci işletim sistemi. Bu iki işletim sistemi türünün güvenlik ve uyum açısından yüksek performans verecek şekilde seçilmesi mantıklı olacaktır.

3.6 Fiziksel Altyapı ve Donanım

Fiziksel altyapı konusu oldukça geniş bir yelpaze şeklinde karşımıza çıkmaktadır. Bu yelpazenin içerisinde tüm donanım alt yapısının ne şekilde seçilirse seçilsin olmazsa olmazı yüksek güvenliğe katkı sağlaması ve uyumlu çalışmasıdır. Donanım üreticilerinin çok çeşitli olması alt yapı kurulumu sırasında kararsızlıklar yaşanmasına neden olmakla birlikte maliyet açısından bakıldığında avantaj sağlayabilir.

Kurumsal hafızanın korunması adına fiziksel altyapı seçilirken dikkat edilmesi gereken önemli parametrelerden bazıları: güvenlik seviyesine katkısı, sağlamlık, uzun süre çalışabilirlik, güncellenebilirlik, kullanılabilirlik, performans, standartlara uygunluk olarak sıralanabilir. Bu parametrelerden maksimum faydayı sağlayan donanımı kurumun imkânları ölçüsünde kullanmak kurumsal hafızanın korunmasına önemli katkı sağlayacaktır.

Güvenliği sağlamada ve bir güvenlik ihlali anında veya acil durumda yapılabilecekler donanımın özellikleri ile sınırlı olacağından bu özellikler hareket kabiliyetini etkileyecektir.

4. Kurumsal Hafızayı Tehdit Eden Unsurlar

Günümüzde özellikle internet hızındaki artışla birlikte bilgiye yetkisiz erişme, kaçırma, bozma, kullanılamaz hala getirme gibi güvenlik açıklarına neden olan aktivitelerin gerçekleşme hızları da artmıştır. Kurumsal bilgilerin, bilgi paylaşımını temel alan faydalı bir girişimle dış dünyaya internet üzerinden açılması paylaşımı artırmakla birlikte, paylaşma şekli ve yöntemindeki yanlışlıklardan dolayı saldırganlar tarafından kötüye kullanılarak istenmeyen güvenlik ihlallerine neden olabilmektedir.

Kurumsal hafızanın saklandığı ortamlarda üçüncü bölümde bahsedilen konuların tamamının veya bir kısmının sağlanamaması başlı başına bir tehdit unsurunu kendiliğinden ortaya çıkarmaktadır.

Kötü niyetli saldırganların, doğrudan veya yazılımlar aracılığı ile dolaylı olarak gerçekleştirdiği bozucu, erişimi sekteye uğratan, bilgi kaçağına, bilginin bütünlüğünün bozulmasına yönelik her türlü faaliyet kurumsal hafızayı tehdit eden bir durumdur.

Bir diğer tehdit unsuru ise kurumsal hafızanın korunmasını sağlayan sistemlerin üçüncü bölümde belirtilen başlıklar dâhilinde değerlendirilmeden kurulmasıdır.

Fiziksel ortam açısından bozucu tehdit unsurları ise;

1- Sıvı maddeler
2- Aşırı ısınma
3- Elektrik dalgalanmaları, kısa devreler vb.
4- Çarpma, düşürme vb. şok dalgaları (Açık bilgisayarlar!)
5- İletken özellikli tozlar.

olarak sıralanabilir. Özellikle kurumsal hafızanın tutulduğu ortamların uluslararası standartları yerine getirecek şekilde inşa edilmesi son derece önemlidir. Geçici olarak yerleşim sağlanmış ise en kısa sürede standartlara uygun ortamlara taşınmalıdır.

5. Çözüm Önerileri

Kurumsal hafızanın korunmasında sistemi oluşturan başlıkların gerçekleştirilmesine ve sağlamlaştırılmasına yönelik olarak yapılması gereken iş ve işlemler birer süreç olarak düşünülmeli ve her biri kendi alanında uzman kişilerce ve toplantılar düzenlenerek karşılıklı görüş birliğine varıldıktan sonra hayata geçirilmelidir. Sistemler ve sisteme dâhil olan bilgiler her gün değişebilen bir yapıya sahip olduğundan alınan kararlar daha sonra ve düzenli aralıklarla mutlaka gözden geçirilmelidir. Buradan hareketle kurumsal hafızanın koruma yapısının çekirdeğini oluşturan ve alınması gereken önlemler şu şekilde sıralanabilir.

- Güvenlik duvarı mutlaka olmalı ve kurum ihtiyaçlarına göre ayarlanmalıdır.
- Kurumlarda mutlaka "Güvenlik Politikası" oluşturulmuş ve uygulanıyor olmalıdır.
- Kurum içi bilgisayarlarda USB, CD, Network'den Boot işlemi kapatılmalı ve bu işlemler sadece yetkililerce yapılabilmelidir, ayrıca BIOS[2] girişleri şifrelenmelidir.
- Bilgisayar vb. cihazlara program yüklemesi sadece yetkililerce yapılmalıdır ve yetkililer şifre vb. önlemlerle bunu kontrol altına almalıdır.
- Kurumların lisanslı antivirüs programları olmalı ve antivirüs programı olmayan bilgisayarlarda yüklenene kadar hiçbir işlem yapılmamalıdır.
- Güvenlik düzeyi yüksek verilerin bulunduğu sistemlere dijital imza, parmak izi veya sms mesajı ile girişler yapılabilmelidir.
- İnsan kontrollü ancak otomatik çalışan yedekleme sistemleri kurulmalıdır. Bununla birlikte yedekler, deprem vb. durumlara karşı farklı coğrafi bölgelerde de depolanmalı, yedeklerin hangi zamanda alındığı ve neyin yedeği olduğu mutlaka etiketlenmelidir.
- Personele özellikle "güvenlik önlemlerini sorgulayarak inisiyatif alıp bazı kuralları esnetmemeleri" alışkanlığı kazandırmak için somut örneklerle konu anlatılmalıdır. Kurumun güvenlik politikasını benimsemeleri ve uygulamaları için gerekli bilgilendirmeler yapılmalıdır. Ayrıca yeni tehditlere karşı değişen-eklenen, önlemler olursa bilgilendirme yapılmalıdır.

6. Sonuç

Sonuç olarak, kurumsal hafızanın korunması için tesis edilen sistemlerin taşıması gereken özellikler düşünüldüğünde bu özellikleri sağlamak için çok sayıda parçanın bir arada eksiksiz ve uyumlu çalışması gerektiği görülür. Bu zor, büyük ve dikkat isteyen bir organizasyondur. Bu sürecin tamamlanmasından sonra işler halde çalışmaya başlayan sistem ise kendi başına terk edilmemeli sistemden sorumlu bir ekip ile kontrol ve güncellemeler sürekli yapılmalıdır. Kurumların kendi öz kaynakları içerisinde bulunan veya dâhil edilecek ve eğitilecek personel ile bu işlemleri yürütmesi sistemin işlerliği açısından son derece önemlidir. Hiçbir sistemin %100 güvenli olmadığı söylenegelse de bu orana yaklaşmanın imkânsız olmadığı bilinmelidir. Bu çalışmada bahsedilen unsurlar ve gerekliliklerin her biri kurumların güvenliğine az veya çok mutlaka katkı sağlayacaktır.

---

[2] BIOS (Basic Input Output Systems): Bilgisayarlarda donanımları ayarlayan ve elektronik olarak çalışır hale getiren temel sistem; anakart üzerinde bulunan bir çip.

Güvenliğin temelinde esasen; itina, dikkat, önemseme, süreklilik ve özveri vardır. Bu düşüncelerle kurulmuş olan uzman bir ekibin bilgi ve tecrübesi donanımla birleştiğinde en yüksek seviyede güvenlik sağlanabilir.

Kaynakça

Bishop, M. (2003). What is computer security? *IEEE Security & Privacy Magazine*, *1*(1), 67–69. http://doi.org/10.1109/MSECP.2003.1176998

Brookshear, J. G., ve Brylow, D. (2014). *Computer Science: An Overview*. Addison-Wesley Longman Publishing Co., Inc. Retrieved from https://books.google.com.tr/books?id=aVnDCwAAQBAJ&dq=Computer+Science:+An+Overview&hl=tr&sa=X&ved=0ahUKEwiFyJDt2fzWAhVpIMAKHf70BWoQ6AEIJjAA

Dieng, R., Corby, O., Giboin, A., & Ribière, M. (1999). Methods and tools for corporate knowledge management. *International Journal of Human-Computer Studies*, *51*(3), 567–598. http://doi.org/10.1006/ijhc.1999.0281

Zhao, G., Hu, X., Li, Y. ve Du, L. (2009). Scheme for digital documents management in networked environment. In *2009 IEEE International Conference on Network Infrastructure and Digital Content* (pp. 995–998). IEEE. http://doi.org/10.1109/ICNIDC.2009.5360955

Lehner, F., & Maier, R. (1998). Organisational Memory Systems Application of Advanced Database and Network Technologies in Organisations. *AMCIS 1998 Proceedings*, 202.

Munier, M. (2011). A Secure Autonomous Document Architecture for Enterprise Digital Right Management. In *2011 Seventh International Conference on Signal Image Technology & Internet-Based Systems* (pp. 16–23). IEEE. http://doi.org/10.1109/SITIS.2011.37

Rhodes-Ousley, M. (2013). *Information Security The Complete Reference, Second Edition*. Mcgraw-hill. Retrieved from https://books.google.com.tr/books?id=FdrdCMvfEe8C

Stallings, W. (2011). *Network Security Essentials: Applications And Standarts* (4th ed.). New York, USA: Prentice Hall.

Stallings, W. (2012). *Operating Systems: Internals and Design Principles*. (M. H. Hirsch, Ed.) (7th ed.). New Jersey: Prentice Hall.

Stein, E. W. (1995). Organization memory: Review of concepts and recommendations for management. *International Journal of Information Management*, *15*(1), 17–32. http://doi.org/10.1016/0268-4012(94)00003-C

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks. *World Wide Web Internet And Web Information Systems*, *52*(169), 349–351. http://doi.org/10.1016/j.comnet.2008.04.002