Kurumunuzun Etkin bir Veri Silme Stratejisi ile Korunması;

BT Varlıklarınızın Mülkiyeti Değiştiğinde Hassas Bilgilerin Ortadan Kaldırılmasını Güvence Altına Alan Adımlar

Blancco Beyaz Kitap

Verilerin Yanlış Şekilde Silinmesi Ciddi Ticari Riskler Doğurabilir

Bir kurum hiçbir zaman taşınmaz ve kaza sigortası olmaksızın faaliyetlerini yürütmeyi düşünmez. Bunun finansal, yasal ve kamuoyu ile bağlantılı riskleri oldukça büyüktür. Ama, aynı kurumlar etkin bir veri kaybı stratejileri olmaksızın her gün faaliyet gösterirler.

Peki bunun riski nedir? Teknoloji sektörünün tanınan bir yayında yer alan aşağıdaki senaryoyu gözünüzün önüne getirmeye çalışın:

"Idaho'da yerleşik bir enerji şirketi eBay'de satılmış olan çok sayıdaki silinmemiş disk sürücüsünün izini sürmeye çalıştığında kendini çok tedirgin edici bir durumda bulmuştu. Sürücülerde çalışanlara ait gizli bilgiler, müşterilerle yapılan görüşmeler ve şirketin müseccel bilgilerinin yer aldığı notlar bulunuyordu. Şirket yaklaşık 230 SCSI sürücünün geri kazanımı için dışarıdan bir taşeron tuttuğunu söylüyordu. Taşeron, online ihale web sitelerini kullanarak sürücülerin 84 tanesini 12 farklı muhataba satmıştı."

Bunun gibi durumlara maalesef çok sık rastlanır olmuştur. Hızla gelişen teknolojik yenilikler BT donanımlarının artan bir hızla eskimiş kabul edilmesine yol açtıkça, PC'ler, sunucular ve belleklere yönelik ikincil piyasalar, yanlış şekilde silinmiş olan sabit disklerin ticari ve kişisel verileri elde etme ve bunları istismar etme çabasındaki teknoloji hırsızları için adeta bir cennete dönüşmektedir.

Şirketler tarafından milyonlarca sabit disk ticari verileri silmek için kullanılan geleneksel çabalar her yıl çoğunlukla başarısız olmakta ve verilerin kötü niyetli kişilerce yeniden diriltilmesine yol açmaktadır. Dahası, elden çıkarmadan önce sabit diskleri silmiş olduklarını iddia eden pek çok üçüncü taraf satıcı da verilerin eksiksiz silinmesi işini titizlikle gerçekleştirmemektedir.

Buna rağmen, 2005 yılında yapılan bir IDC araştırmasına **göre ticari kuruluşların sadece %37'sinin resmi bir PC geri kazanım ve yaşam sonu varlık politikası bulunmaktadır**. Buna ilaveten, operasyonel veri merkezleri bulunan ve bu süreçleri sunucu ve bellek güruhlarıyla idare eden kurumlar için bu çok daha dikkat gerektiren bir husustur.

Rapor verilerin imha edilmesinde de benzer bir oran olduğuna dikkat çekmektedir.

Müseccel bilgilerin yanlış ellere geçmesinin yarattığı mahsur ve utancın yanı sıra, satış ve imha öncesinde ticari verilerin etkin bir şekilde silinmemesinin beraberinde getirdiği daha da ciddi sonuçları bulunmaktadır. Kurumlar, kimlik/özel hayat davaları, federal kanunların ihlali, çevresel zarar, fikri mülkiyet haklarının ihlali, ticari stratejilerin ifşası, yazılım lisans anlaşmasına itaatsizlik (lisans harmanlama) ve olumsuz kamuoyu gibi oldukça zarara uğratıcı yasal, finansal ve halkla ilişkilerle ilintili risklere maruz kalabilirler.

Dolayısıyla, her bir BT Yöneticisinin, hassas verilerin, elden çıkarılmadan önce tüm bellek ortamlarından etkin bir şekilde silinmesini garanti altına alan resmi süreçlerin geliştirilmesinde, dokümanlaştırılmasında, duyurulmasında ve uygulanmasında kritik sorumlulukları bulunmaktadır.

Okumakta olduğunuz bu beyaz kitap, kurum BT yapılarını resmi veri silme politikalarının temel unsurları hakkında eğitmede ve kendilerini eksik veya uygun olmayan şekilde silinmiş verilerin yaratabileceği maliyetli yasal, denetsel, finansal ve halkla ilişkilerle ilgili kabuslardan etkin bir şekilde korumalarına yardımcı olmak üzere hazırlanmıştır.

Düzgün olarak tasarlanmamış bir veri elden çıkarma süreci bir kurumu çok çeşitli yasal, finansal ve halkla ilişkiler risklerine maruz bırakabilir.

Verilerin Silinmesi Neden Bu Denli Önemlidir?

Bilgi varlıklarının büyük bir kısmı, kurumların yasal olarak, ahlaki açıdan ve emanetçi sıfatıyla sorumluluğunu taşıdıkları gizli bilgilerden oluşmaktadır. Açık ve net bir veri silme politikası bulunmayan şirketler ya da varlık imha süreçleri sağlıksız bir şekilde tasarlanmış şirketler kurumlarını pek çok riske maruz bırakabilirler; bunlar arasında:

Müşteri, Ortak ve Çalışanların Güven Riski

Müşteri ve çalışanlar, bir kurumla kurdukları çalışma ilişkisinin bir parçası olarak kişisel ve ticari bilgilerinin güvenliğini kuruma emanet ederler. Bir BT varlığının veya bellek aygıtının elden çıkarılmasıyla söz konusu bilgilerin etkin bir şekilde silinememesi marka ve/veya şirketin imajına zarar verebilir, hisse senedi fiyatlarının düşmesine, müşterilerin ve iş ortaklarının kaybedilmesine ve olumsuz kamuoyu oluşmasına yol açabilir. Şirket çalışanlarının sık değişmesine de neden olabileceğinden şirketin günlük faaliyetleri sekteye uğrayabilir, kurum içi bilgi güvenliği olumsuz etkilenebilir.

Uyum/Denetim Riskleri

Katı sektör standartları ve hükümetlerce yapılan düzenlemeler, kurumlara gizli bilgilerin yetkisiz bir şekilde ifşa edilmesi riskini ortadan kaldırılması yönünde sorumluluk getirmektedir. Düzenlemeye tabi sektörlerde faaliyet gösteren kurumların gizli bilgilerin sızmasını engelleyecek adımları aldıklarını kanıtlamaları ve eksiksiz bir denetim kaydına sahip olmaları gerekmektedir. Konu ile ilgili düzenlemeler arasında HIPAA (Health Insurance Portability and Accountability Act), FACTA (Fair and Accurate Transactions Act), GLB (Gramm-Leach Bliley), CAL SB1386 (The California Information Practice Act) ve SOX (The Sarbanes-Oxley Act) yer almaktadır.

Düzenlemeye tabi sektörlerde faaliyet gösteren kurumların gizli bilgilerin sızmasını engelleyecek adımları aldıklarını kanıtlamaları ve eksiksiz bir denetim kaydına sahip olmaları gerekmektedir.

Dava/Yasal Riskler

Kimlik hırsızlığı en çok büyüyen suç türlerinden biridir. Federal Ticaret Komisyonu'na göre, kimlik hırsızlığı, müşterilerin en çok şikayet ettiği konu olmuş ve 2006 yılında yapılan şikayetlerin %36'sına ulaşmıştır. Dikkatsizce hurdaya çıkarılan ve kredi kartı detayları, sosyal güvenlik numaraları ve iletişim bilgileri gibi gizli verileri içeren bir sabit disk kolaylıkla kimlik hırsızlığına yol açabilmekte ve kurumu olumsuz kamuoyu ve maliyetli davalarla baş başa bırakabilmektedir.

Yazılım Lisanslama Riskleri

BT varlığı el değiştirdiğinde sabit disk üzerinde kalan uygulama ya da sistem yazılımı yazılım geliştiricisinin site lisanslama koşullarını ihlal edebilir. Bundan başka, bir sunucunun bir başka departman ya da bölüme yeniden tahsis edilmesi de yazılım lisansına yönelik bir ihlal durumu oluşturabilir ve maliyetli cezalar getirebilir.

Veri Silme Yöntemleri

Kurumlar geleneksel olarak veri silme olayına taktiksel, bir defaya mahsus veya "nokta-çözüm" perspektifinden yaklaşmışlardır. Ancak maalesef, veri silmeye ilişkin karmaşık unsurlar, günümüzün kurum ticaret ortamının gerektirdiği pek çok önemli alanda çoklu kararlar almayı içeren daha stratejik bir yaklaşım gerektirmektedir. Bu unsurlarla ilgili avantajlı ve dezavantajlı durumlar aşağıda ele alınmaktadır:

Fiziksel İmha- Verilere erişimin engellenmesi amacıyla gerçekleştirilen fiziksel imhada sabit disk ve bellekler imha edilmektedir. Bu ise ya sabit diskin ince şeritler halinde kesilmesi ya da sabit disk tablasına bir dizi delik açmak yoluyla yapılmaktadır. Bu yaklaşım verilerin her zaman silinmesiyle sonuçlanmamakla birlikte sabit disk çalışmaz kılmakta ve böylelikle sıradan yöntemlerle veri geri kazanımını engellemektedir.

Avantajları- Bu yaklaşım, sürecin düzgün bir şekilde tamamlanması halinde verilerin bilahare geri kazanımını önleyen etkin bir yoldur. Bu yöntemle fazla miktarda medya tek seferde imha edilebildiği gibi manyetik sabit disklerin yanı sıra manyetik diskler, CD'ler, DVD'ler veya sökülebilir sürücüler gibi farklı medya türleri aynı zamanda yok edilebilir.

Dezavantajları – Fiziksel imha yönteminde sabit diskin hurda değerinin geri kazanımı ihmal edilmektedir; dolayısıyla bu yaklaşım, kurum içerisinde tekrardan kullanılabilecek ya da ikincil piyasada satılabilecek nitelikte pahalı, geniş kapasiteli sürücüler için geçerli değildir. İmha için gerekli olan ekipman maliyeti nedeniyle, imha işlemi genellikle bir taşerona verilmektedir ki bu da doğal olarak gizli verilerin teşhir edilme riskini artırmaktadır. İmha esnasında EPA düzenlemelerini muhtemelen ihlal edecek düzeyde bir zehirli enkaz oluştuğu için fiziksel imha çevresel bir risk de yaratmaktadır. Tüm bu dezavantajların yanı sıra, imha sürecinin düzgün şekilde gerçekleştirilememesi durumunda da bellek medyasının kalan kırıntıları üzerinden verileri geri kazanmak mümkün olabilmektedir.

Manyetik Etkinin Nötrleştirilmesi (Degaussing) – Bir sabit diskin manyetik etkisinin nötrleştirilmesinde kuvvetli elektromanyetik alanlar kullanılmakta olup, ideal koşullarda sürücü üzerinde manyetik olarak kaydedilmiş tüm veriler imha edilmekte ve sürücü çalışamaz kılınmaktadır.

Avantajları-"Degaussing" adı verilen bu süreç oldukça hızlı olup sabit disk veya diğer manyetik medya üzerindeki tüm verilerin imha edilmesini sağlamaktadır. "Degaussing" makinasının satın alınması çoğu durumda tek seferlik bir yatırım olduğundan maliyetleri hafifletmektedir.

Dezavantajları – “Degaussing” işlemi her ne kadar eski sürücü teknolojilerinin imha edilmesini garantilemekteyse de, verilerin eksiksiz olarak silindiğinden emin olmak için daha kalın muhafazaya sahip yeni sürücüler için daha kuvvetli elektromanyetik alana gereksinim duyulmaktadır. Sürücü tasarımlarındaki değişikliklerden ötürü maalesef “degaussing” işleminin tüm verileri noksansız sileceğini ve kurumu herhangi bir güvenlik ihlalinden koruyacağını garanti eden tekdüze bir yol bulunmamaktadır.

Ayrıca, bu seçenek sadece manyetik medyalarda kullanılabilmekte olup, ilgili süreçler dikkatlice yerine getirilmediğinde tüm verilerin güvenilir şekilde silinememesi söz konusu olmaktadır. Manyetik alanların doğası gereği, yakın bölgedeki aksam ve ekipmanın da zarar görmesini engellemek için özen gösterilmesi gerekmektedir.

Sürücünün Yeniden Formatlanması- Yeniden formatlamanın pek de etkin olmayan bir veri silme yöntemi olduğuna dair gitgide artan farkındalığa rağmen, pek çok kurum bu yöntemin içerdiği güvenlik risklerine gözlerini kapatmaktadır.

Avantajları- Veriler tamamen silinmediği için bu yöntemin sağladığı hiçbir avantaj bulunmamaktadır.

Dezavantajları – Tüm “Sil” ve “Format” komutları sürücünün sadece Dosya Tahsis Tablosunu (File Allocation Table-FAT) değiştirir ve gerçekte hiçbir veriyi silmez. Silinen sadece veri dosyalarına işaret eden adres tablolarıdır. Veriler hala bozulmamış olarak durur ve Internet’te bile satılmakta olan yazılım hizmetlerinin kullanılması yoluyla kolaylıkla geri kazanılabilir.

“Silinen” verilerin üzeri tamamen yeni verilerle kapatılmadıkça, veriler orada durur ve kimlik hırsızlığı, yasal işlem ve davalar ve muhtemel hapis açısından önemli boyutta güvenlik riski barındırırlar. Sonuç olarak, verilerin bu yöntemle imha edilmesinden kesinlikle uzak durulmalıdır.

Format komutları sürücünün sadece Dosya Tahsis Tablosunu(File Allocation Table-FAT) değiştirir ve gerçekte hiçbir veriyi silmez. Veriler hala bozulmamış olarak durur ve satılmakta olan ticari yazılım hizmetlerinin kullanılması yoluyla kolaylıkla geri kazanılabilir.

Üstüne Yazma Yazılım Çözümleri- Mevcut bilgiler üzerine veri yazılmasına imkan veren yazılım çözümleri 1’ler ve 0’lar kombinasyonu kullanılarak sürücü sektörlerinin her biri üzerine anlamsız verilerden oluşan yazı kalıpları yerleştirilmesinden oluşan bir süreçtir.

Avantajları- Bu seçenek verileri kalıcı olarak imha etmenin en etkin ve uygun yoludur. Cihaz bir kez silindi mi, varlığın fonksiyonel ve yeniden pazarlanma değeri korunduğundan yeniden kullanılabilir ya da yeniden satılabilir. Bazı durumlarda, araç, şebeke üzerindeki belli birtakım bilgisayarları ya da sürücüleri hedef alacak şekilde konuşlandırılabilir. Düzgün olarak tamamlanan süreçlere teyit eden raporlamalar yaratabildiği gibi yazılım tarafından üstüne yazılamamış olan bozuk kesimleri listeleyen bir hata kütüğü de oluşturabilir. Raporlar uyum gereksinimlerini yerine getirmekte ve sıklıkla sürücü seri numarası, veri silme boyutu, silme prosedürünün, teknisyenin adı ve silme sürecinde yaşanan hataları gibi bilgileri de içermektedir.

Dezavantajları- Pek çok kurum daha halen daha eski standartlara ve üç ila yedi üzerine yazmadan sonrasına yönelik önerilere bel bağlamış durumdadır. Bunlar yetersiz yazılım araçlarıyla bir araya geldiğinde standart bir PC'nin silinme sürecinin saatler sürmesine yol açmaktadır. Buna ek olarak, üstüne yazma programlarının hepsi de eksiksiz bir güvenlik sunmamaktadır. Örneğin, Internet'ten rahatça erişilebilen ücretsiz üzerine yazma araçları, saklı/kilitli dizinler veya sürücünün yeniden eşleşen (remap) sektörlerini içerebilecek sabit diskinin tamamına erişememektedir. Tamamlanmış/eksik sonuçlar olması durumunda, verilerin bir kısmı el sürülmemiş halde kalabilir ve güvenliği tehlikeye atar. Dahası bellek medyası hasar görmüşse veya üzerine yazılamıyorsa bu çözümler kullanılamaz.

Donuk Depolama- Pek çok şirket güvenlik ihlali endişesi nedeniyle karar verememekten ya da alternatifler hakkında bilgi sahibi olmamaktan ötürü, verilerin yanlış ellere düşmemesini garantilemek için sabit diskleri ve bilgisayarlarını depolamaktadır.

Aslında, kurumların büyük bir kısmı depolamayı birincil bir varlık elden çıkartma yöntemi olarak seçmektedir. BT konferansına katılan 320 BT profesyoneline yönelik olarak Gartner Research tarafından gerçekleştirilen bir araştırmada, **depolamanın**, demode olmuş/eskimiş PC ve sunucularla baş ederken **sıklıkla başvurulan üçüncü yöntem** olarak benimsendiği ortaya çıkmıştır. Araştırmaya katılan şirketlerin yaklaşık ¼'ü, demode olmuş PC ve sunucularının %30'undan fazlasını depoladıklarını belirtmişlerdir.

Avantajları- Depolanan ekipman ve sabit diskler diğer departmanlara hızlı ve kolay bir şekilde yeniden yönlendirilebilmekte ve böylelikle kurulum zamanı ve iktisap maliyeti düşürülebilmektedir.

Dezavantajları- Bir bilgisayar ekipmanı depolandığında, çalışanların söz konusu ekipmanı-özellikle de sabit diski aşırma/yürütme eğilimi vardır, böylelikle depolamayla asıl önüne geçilmek istenen riskin ta kendisi-güvenlik riski- yaratılmaktadır. Teknoloji ekipmanlarının hızlı değer kaybetme doğasından ötürü, depolanan ekipmanların negatif bir değer getirmesi de mümkün olmaktadır. Dahası, BT varlığının transferi sonrasında, daha öncesinde kurulmuş olan uygulama ve sistem yazılımları kaldırılmazsa, şirket kendisi yazılım lisansının koşullarına uyum sağlamayan bir konumda da bulabilir.

Araştırmaya katılan şirketlerin yaklaşık ¼'ü, demode olmuş PC ve sunucularının %30'undan fazlasını depoladıklarını belirtmişlerdir. Gartner Research "BT Varlık Yönetimi ve Varlık Elden Çıkarma" Kasım 2005

Şekil 1'de veri güvenlik önlemlerinin avantaj ve dezavantajlarını gösteren bir matriks yer almaktadır:

Şekil:1 Veri Güvenlik Önlemleri Matrixi

Avantaj	Hiçbir Şey Yapmamak	Sürücünün Formatlanması	Fiziksel İmha	Üzerine Yazma Yazılımı	Depolama
Rahatlık	Yok	Yok	Var	Var	Yok
Azalan Risk	Yok	Yok	Var	Var	Yok
Denetlenebilir Uyum	Yok	Yok	Var	Var	Yok
Kanıtlanmış Çözüm	Yok	Yok	Var	Var	Yok
İtibar	Yok	Yok	Kesin Değil	Var	Yok
ROI (Return on Investment, Yatırımın Getirisi)	Yok	Var	Kesin Değil	Var	Yok
Geleceğe Yönelik Kanıt	Yok	Yok	Yok	Var	Yok

Veri Silme Yöntemleri

Bir yandan bilgi dolandırıcılığının taşıdığı riskleri azaltırken diğer yandan da devletlerin getirdiği düzenlemelere uyum sağlamada, gizlilik hassasiyetlerine ve fikri mülkiyet hakları gibi hususlara özen göstermede tüm şirketlerin etkin birer veri fire önleme politikası tasarlamak ve elden çıkarma veya yeniden satışa yönlendirilmiş BT varlıklarına ilişkin veri silme prosedürleri oluşturmak gibi sorumlulukları bulunmaktadır.

Kurum çapında veri silme politikası oluşturmak için atılacak yedi önemli adım aşağıda yer almaktadır:

1.Gerçekleştirilmesi En Olanaklı Çözümü Tespit Edin- Her şirketin veri silme politikası, şirketin büyüklüğü, veri silme ve elden çıkarma sıklığı ve özel birtakım sektör gereklilikleri gibi çeşitli faktörlere dayalı olmalıdır. Örneğin, küçük bir işletme için pahalı veri silme ekipmanı satın almak finansal anlamda akıllıca olmayabilir. Öte yandan, şirketi sıklıkla güvenlik riskine maruz bıraktığından büyük bir kurum için de demode olmuş binlerce bilgisayarı depolamak asla mantıklı değildir. En etkin çözümü tespit etmek için, işletmeler mevcut kaynaklarını kullanmalı ve kaynaklarının eksik olduğu alanlarda dışarıdan bilirkişi görüşü almalıdır. Kurumların aynı zamanda organizasyonel büyüme ve/veya şirket satın alma gibi gereksinimleri ve uygulama seçeneklerini değiştirecek gelecek ihtiyaçları için de plan yapmaları gerekmektedir.

2. Maliyetleri Hesaplayın ve Bir Bütçe Oluşturun- Çoğu kuruluşun BT ekipmanı ve hizmetleri için ayırdığı bir bütçe bulunurken, pek azının veri silme ve varlık elden çıkarma için bir bütçesi bulunmaktadır. Değişik pek çok alternatif olmakla beraber bunların her biri maliyet taşıyan riskler içermektedir. Etkin bir veri silme stratejisi uygulamak suretiyle, bir şirket BT ekipmanlarını satın aldığı tarihi izleyen iki ila üç yıl içerisinde ekipmanları geri satarak ekipmanların kalan değerini sıklıkla elinde tutabilir. BT varlıkları genel olarak üç yıl içerisinde tam olarak amortize edilirler. Kalan yeniden pazarlama değerinin (remarketing value-RMV) amortizasyon tablosuyla bir ilgisi bulunmamaktadır.

Ancak, 3 ila 5 yıl arasında bir noktada (sunucu ve bellekler değerlerini daha uzun süre için korurlar) RMV sıfıra ulaşır (ancak elden çıkarma maliyetleri yerinde kalır) ve varlık artık bir yükümlülük haline gelir.

Çoğu kuruluşun BT ekipmanı ve hizmetleri için ayırdığı bir bütçe bulunurken, pek azının veri silme ve varlık elden çıkarma için bir bütçesi bulunmaktadır.

3.Rolleri ve Sorumlulukları Dağıtın- Nihai veri silme kararı nerede alınacak? Bu kararı "Başkan seviyesinde" bir yönetici mi alacak, yoksa BT direktörü mü ya da Satın Alma Müdürü mü? Veri silme teknik veya operasyonel bir mesele değildir, aslında bir risk ve yükümlülük meselesidir. Sonuç olarak, karar vericinin kurum risk yöneticisi veya güvenlik mimarı gibi, bir şeyler ters gittiğinde bundan en çok etkilenecek birey olması gerekmektedir. Her iki durumda da, veri silme, bir sahibinin bulunması gereken bir süreçtir. İlave personel konuları, veri silme için gereken personel sayısının ne olduğunun, bunların nerede oturtulacağının ve İnsan Kaynaklarının oynayacağı rolün tespit edilmesini içerir. Personel maliyetleri önemli boyutta olabileceğinden, personel gereklilikleri teknik ve prosedürle ilgili hususlarla birlikte ele alınmalıdır.

4. Elden Çıkarma Mahallini Seçin- Veri silme işleminin gerçekleştirildiği tesis silme sürecinin hem kalitesini hem de güvenliğini etkileyebilir. Örneğin, hassas verilerin kurum dışına çıkmadığından emin olunacak şekilde yerinde yapılan veri silme işlemi en güvenli seçenektir. Veri silme işlemi için şirket dışında bir mekanın ya da üçüncü bir tarafın tesisinin kullanılması halinde sürece, doğrulanabilir tesis güvenliği ve dokümantasyon gibi başkaca adımlar eklenmektedir. Sorulması gereken önemli sorular arasında: Söz konusu mahal silme süreçlerinde yer alan adımları detaylandıran bir İş Beyanı (Statement of Work-SOW) sağlıyor mu? Düzenlemelere uyum çerçevesinde yapılan raporlamalara ilişkin her hangi bir sertifika veriliyor mu? Tespit edilen çalışma alanlarına gözetim amaçlı güvenlik kameraları yerleştirilmiş mi? Taşıma esnasında oluşabilecek yetkisiz erişimin engellenmesini teminen mühürlü ve sağlam konteynerler kullanılıyor mu? Yerinde veya başka mahaldeki tesislerin kullanıldığı her iki durum için de etkin seçenek birleşik bir yaklaşım benimsemektir. Örneğin, bir şirket, işletmeye ait en hassas verilerin tutulduğu bellek medyaların yerinde silinmesini benimserken daha az hassas bilgilerin bulunduğu medyanın başka mahalde silinmesi ver elden çıkarılması yöntemini kullanabilir.

5.İşin Ehli /Kalifiye bir Hizmet Sağlayıcısı Seçin- Veri silmeden sorumlu kişi ya da şirketi seçerken dikkate alınması gereken iki faktör kontrol ve maliyettir. Şirket çalışanlarının kullanıldığı veya dışardan tutulan hizmet sağlayıcının şirket mahalline getirildiği politikalar en yüksek derecede kontrol sağlamakla beraber yüksek maliyet içermektedir. Medyanın başka bir lokasyona taşınması daha düşük bir maliyet içermekte ancak daha düşük seviyede kontrole imkan vermektedir. Her iki seçenek de geçerlidir ancak seçeneğin içerdiği risk ile sunduğu maliyet tartılmalıdır.

6.Masaüstü/Veri Merkezi Araç Yönetimini Planlayın- Veri merkezi ekipmanı masaüstü PC'lerden ve dizüstü bilgisayarlardan farklı bir şekilde kurulur, kullanılır ve yönetilir. Sonuç olarak, silme işlemi için belirlenmiş bellek medyasının yerine koymak üzere ağ sunucusu veya array'i gibi ekipmanlardan bellek aygıtlarının çıkartılması temel/asli iş fonksiyonlarını etkileyebilir. Hayati öneme sahip uygulamaları çalıştıran sunucular veya bellek array'leri, tekrar işler hale gelebilmeleri için

tamamlanması gereken maliyetli ve zaman alıcı süreçler olmaksızın, öyle hemen devre dışı bırakılıp bunların faaliyetlerine son verilemez. Söz konusu sürecin içerdiği külfetlerin boyutu nedeniyle, görevi yerine getirmeye uğraşan tecrübesiz personelin kritik iş fonksiyonlarında yol açabileceği kesinti riskini üstlenmektense, kalifiye uzmanları dışardan bu iş için görevlendirmek çok daha maliyet etkin olabilir. Karar vermeden önce şu soruyu sorun: Şirket çalışanları söz konusu görevi yerine getirebilecek yeteneğe haiz mi ve işe yönelik mevcut öncelikleri dikkate alındığında sürece yeterli zaman ayırabilecek durumdalar mı? Dışardan bu iş için tutacağınız uzmanlar çok sınırlı veya hiçbir kesintiye uğratmadan süreci hızla tamamlayabileceklerse, söz konusu hizmeti dışarıdan almak daha maliyet etkin bir seçim olabilir mi? Hizmeti dışardan almakla daha etkin sonuçlar mı elde edebilirsiniz yoksa ilave ve daha maliyetli sorunlar mı yaratırsınız?

Cihazların ağdan ayırılıp, silme işlemi için belirlenmiş bellek medyasına erişiminde izlenen yol asli iş fonksiyonlarını etkileyebilir.

7. Denetsel ve Raporlama Gerekliliklerini Araştırın- Düzenlemeye tabi bir sektörde faaliyet gösteren ve hassas bilgileri elinde tutan kamu ve özel kurumlar, varlık elden çıkarımı ve veri silinmesi ile ilgili bir işlem geçmişi raporu/denetim kaydı yaratmanın ve federal ya da devlet düzenlemelerine uyumlu raporlar üretmenin gerekliliği konusunda hemfikir olmalıdırlar. Raporlar elden çıkarılan ya da silinen kalemleri, bunların seri numaralarını, verilerin ne şekilde silindiğini ya da varlıkların ne şekilde elden çıkartıldığını ve elden çıkarma prosedürlerinin ne olduğunu göstermelidir. Kurumsal ölçekte kullanılan üzerine yazma yazılımlarının avantajı bu raporları üretebilmeleri ve kurumları uyum konusundaki yasal davalardan korumada yardımcı olmasındadır.

Kurum Ölçeğinde, Veri Silme Stratejisi Tespit Edilirken Dikkat Edilmesi Gereken Hususlar

Kurumsal ölçekte etkin bir veri silme stratejisini oluşturan pek çok bileşen bulunmaktadır. Veri sızıntılarının önlenmesine ve varlıkların elden çıkarılmasına yönelik politikalar oluşturulurken sorulması gereken kritik sorulardan bir kısmı ve temel kriterler aşağıda yer almaktadır:

- Düzenlemeler- Kurumunuz hangi özel sektör düzenlemelerine tabi ve veri ve BT varlık elden çıkarılmasıyla ilgili olarak bu düzenlemeler neler gerektiriyor?
- Dahili Politikalar- Bu gereklilikleri yansıtan yazılı politikalarınız bulunuyor mu? Kurumunuz bu politikaları etkin olarak uygulayabilecek kapasitede mi?
- Denetimle İlgili Faktörler- Mevcut politikalarınız ve uygulamalarınız denetlenebilir halde mi?

Pek çok kurumsal BT departmanı disk yardımcı programlarında bulunan basit üzerine yazma fonksiyonlarını kullanmaktadır. Ancak, bu araçların kurum güvenliğini riske atacak önemli boyutta kusurları olabilmektedir. Kurum ölçeğinde yüksek etkinliğe sahip üzerine yazma yazılımlarının, veri temizleme sürecinde bütünlük sağlanmasını teminen aşağıda yer alan fonksiyonlara ve kapasiteye sahip olması gerekmektedir:

Güvenlik ve Performans:

- Uyumluluk- Sürücü üzerine yüklenen OS ile uyumluluk ya da ondan bağımsız olarak çalışabilme yeteneği

- Bağımsızlık- Temizlenmekte olan sabit disk türünden (mesela Advanced Technology Attachment (ATA)/Integrated Drive Electronics (IDE) ya da Small Computer System Interface (SCSI) türünden sabit disklerin bağımsız olarak çalışabilme yeteneği
- Üzerine Yazma- Herhangi bir Basic Input/Output System (BIOS)'tan veya sistemin sahip olabileceği şirket çapında kapasite sınırlamasından bağımsız olarak sabit disk sürücüsünün tamamı üzerine yazabilme kapasitesi
- Saptama- HPA,DCO gibi kilitli ve saklı sektörleri, yeniden eşleştirilen (remap) sektörleri ve bunun yanında RAID konfigürasyonlarındaki sıcak boş alanlı (hot spare) sabit disklerin silinmesi durumları saptama, raporlama ve üzerine yazma becerisi

Raporlama ve Denetleme

- Sertifikasyon- Kullanıcıya üzerine yazma prosedürün hatasız tamamlandığına dair ibare taşıyan bir silme sertifikasının/raporunun verilmesi
- Donanım Konfigürasyonu-Hayati öneme sahip konfigürasyon bilgileriyle bilgisayar seri numaraları ve varlık etiketlerini tespit etme ve raporlama özelliği
- Lisans Harmanlama-Lisans harmanlama için, örneğin ana SW seri anahtarlarını tespit etme ve raporlama özelliği
- Dijital İmza-Raporun doğruluğunun dijital imzalarla güvence altına alınması

Son olarak, kalifiye bir hizmet sağlayıcının aşağıdaki niteliklere sahip olması gerekmektedir:

- Sigortalanmış olmalıdır (asgari USD 1 milyon)
- İtibarlı olmalıdır ve başarısı kanıtlanmış yazılım ve operasyonel teknikler kullanmalıdır
- Kurum içinde ve destek için sertifikalı mühendisleri bulunmalıdır
- Seri numaraları içeren sertifikalar verebilmelidir
- Silinmiş olan her bir disk için teyit amacıyla silme raporları verebilmelidir,
- Hem yazılım bazlı silme hem de veri imhası için alternatifler sunabilmeli ve operasyon maliyetlerinin azaltılmasını teminen çözümleri birleştirebilme becerisine sahip olmalıdır
- Referans verebilmelidir

Özet

Kurumsal bilgi hırsızlığı ve dolandırıcılığında yaşanan hızlı artış veri silme ve BT varlık elden çıkarma konularını, kurum açısından, kurum ağlarının düzgünlüğü ne kadar önemliyse o kadar önemli hale getirmiştir. BT varlıklar kurumun tesisinden çıktığında işletmeye dair ticari bilgileri düzgün bir şekilde güvence altına alamayan bir kurum, yasal, finansal ve pazarlama ilintili pek çok alanda ciddi ceza riskleriyle karşı karşıya kalır.

Ömrünü tamamlamış BT varlığı ve verilere yönelik sağlıklı ve iyi planlanmış bir politika her kurumun kurumsal bilgi stratejisinin temel bileşeni olmalıdır. Elden çıkarma ve silme yöntemleri sadece fiyatı baz almak suretiyle seçilmemelidir. Farklı elden çıkarma alternatiflerinin hepsinin sunduğu avantajlar ve dezavantajlar bulunduğundan her bir kurumun kendine özgü gereksinimleri dikkate alınarak değerlendirilmelidir.

İyi yapılandırılmış veri silme ve varlık elden çıkarma politikasının işletme açısından en önemli üç avantajı şunlardır:

- **İşletme Riskinin Azaltılması**- İyi planlanmış bir veri silme politikası, işletmeye ait verilerin yanlış ellere düşmesi sonucunda oluşabilecek maliyeti yüksek risklerin oluşma olasılığını, yükümlülükleri, denetsel gereksinimleri ve kamuoyu nezdinde oluşabilecek mahcubiyetleri azaltır.
- **Veri Güvenliğinin Garanti Altına Alınması**- Düzgün şekilde yönetilen bir veri ve varlık elden çıkarma politikası işletmeye ait bilgilerin güvenliğini sağlama almak suretiyle müşteriler, çalışanlar ve iş ortakları arasındaki ilişkiyi korur.
- **Yatırımdan Daha Yüksek Getiri Sağlanması**- Titiz ve düzenli bir veri silme politikası bir kuruma yaşlanan BT varlıklarını güvenli bir şekilde yeniden pazarlama imkanı sunmak suretiyle verilerde sızıntının önlenmesine ve varlık elden çıkarılmasına yönelik politikalarının içerdiği maliyetleri azaltır.

İşletmeler müseccel verilerinin yanlış ellere düşmesinin yaratabileceği risk ve yükümlüklerden kendilerini korumak için resmi bir veri silme politikası oluşturmalı ve uygulamaya koymalı, kendilerine en maliyet-etkin, güvenli ve en iyi korunma seçeneklerini sunabilen kalifiye ve tecrübeli veri silme ve varlık elden çıkarma kaynaklarıyla kendilerini uyumlu hale getirmelidir.

E-Data Teknoloji

Merkez : 0312 472 36 56
İstanbul : 0212 211 28 54