BELEDİYELER İÇİN SİBER GÜVENLİK ÖNERİLERİ

Sparta Bilişim

Sparta Bilişim, kuruluşların siber güvenlik konusunda ihtiyaç duydukları profesyonel hizmetleri sunmak amacıyla 2013 yılında kurulmuştur. Bugüne kadar 200'ün üzerinde kuruluşa sızma testinden, siber olaylara müdahaleye kadar geniş bir alanda hizmet veren Sparta, iş birliği yaptığı kuruluşların mevcut bilgi teknolojileri ve bilgi güvenliği ekiplerinin bir uzantısı gibi çalışmaya özen göstermektedir.

Güvenlik Yaklaşımımız

Eski Yunan'da etrafı surlarla çevrili olmayan tek şehir Sparta'dır. Bunun nedeni kral Agesilaus'a sorulduğunda askerlerinin mızraklarını gösterip "Sparta'nın surları bunlar" dermiş. Kuruluşların siber güvenlik seviyesini artırmak için savunma (firewall, antivirüs, vb.) çözümleri sunmuyoruz. Başta sızma testleri olmak üzere sunduğumuz hizmetler "saldırı" tarafında. Hackerların ve zararlı yazılımların neler yapabileceğini önceden tespit ederek gerekli ve doğru tedbirleri almanızı sağlıyoruz.

Duvar gibi reaktif değil, proaktif güvenlik süreçleriyle hizmet verdiğimiz kuruluşların surlarını sağlamalaştırıyoruz.

İÇİNDEKİLER

Belediyeler Açısından Siber Güvenlik

Siber güvenlik konusunda atılacak adımların saldırgan ve risk odaklı değerlendirilmesi doğru bir yol haritası çizilebilmesi için önemlidir. Dünyada ve ülkemizde kuruluşlar açısından siber risk oluşturabilecek saldırgan profillerine bakacak olursak, bunları 6 gruba ayırmak mümkün olmaktadır:

1. Diğer ülkeler: Yabancı ülkelerin siyasi, ekonomik veya stratejik hedeflerine hizmet eden saldırgan grubudur. Ülke destekli siber saldırgan gruplarının, hedef odaklı yaklaşımları ve sahip oldukları maddi kaynaklar sonucunda ortalamanın üstünde güvenlik seviyesi olan ağ ve sistemlere sızmaları mümkün olmaktadır. Kore, Rusya ve Çin gibi adını düzenledikleri küresel siber casusluk operasyonları ile sıkça duyduğumuz ülkelerin yanında, Lübnan gibi daha küçük ülkelerin de bu kapsamda göz ardı edilmemesi gerekmektedir.
2. Organize suç unsurları: Maddi kazanç beklentisiyle hareket eden gruplardır. Kişisel bilgilerin çalınıp satılması, fidye yazılımlar aracılığıyla para toplanması veya hedef kuruluş kaynaklarının kriptopara madenciliği için kullanılması gibi faaliyetler yürütürler.
3. Hacktivistler: İdeolojik motivasyonu olan bu gruplar, eylemlerini hedef aldıkları kuruluşun idari kararlarını değiştirmek veya küçük düşürmek gibi amaçlarla planlarlar.
4. İç tehditler: Kuruluş bünyesinde çalışan personel tarafından düzenlenen veya desteklenen saldırılar “iç tehdit” olarak değerlendirilmektedir. Kuruluş içerisinde gizli kalması gereken bilgilerin sızdırılmasından sabotaja kadar geniş bir yelpazede eylemler görülebilmektedir.
5. Fırsatçı saldırganlar: Genellikle kendi çevrelerinde isim yapmak isteyen veya bilinen bir açığın var olabileceği sistemleri arayan saldırgan grubudur. Teknik becerileri sınırlı olsa da bilinen bir zafiyetin kuruluş sistemlerinde bulunması halinde etkili olabilmektedirler.
6. Kullanıcı hataları: Kuruluş sistemlerinin kullanıcıları tarafından yapılan hatalar siber güvenlik seviyesini olumsuz etkileyebilmektedir. Bu kategoride yanlış yetkilerin verilmesi, ağ tasarımında güvensiz noktalar veya fabrika çıkışlı kullanıcı hesaplarının kullanımı gibi basit hatalar görülebilmektedir. Personelin kötü niyeti olmamasına rağmen bu hataların sonuçları yıkıcı olabilmektedir.

A.B.D. Güney Carolina Belediyeler Birliği tarafından yayınlanan bir araştırma sonucunda yaşanmış siber saldırıların analiz sonuçlarına yer verilmiştir. Bu rapora göre; belediyeleri hedef alan siber saldırıların %98'i aşağıdaki 4 kategoriye dağılmaktadır:

- Hatalar (%34): Bilgi güvenliği ihlaline neden olan personel hataları
- İç tehdit (%24): Personelin kötü niyeti veya dikkatsizliği sonucunda yaşanan ihlaller
- Dışarıdan yapılan saldırılar (%21): Teknik veya sosyal mühendislik saldırıları sonucunda yaşanan olaylar
- Kayıt/çalıntı (%19): Belediyeye ait varlıkların kaybolması veya çalınması sonucunda yaşanan kayıplar

Genel olarak görülen siber saldırgan profillerine ek olarak belediyeleri hedef alması muhtemel bir saldırganın terör, siber savaş ve casusluk amacıyla hareket etme ihtimali yüksektir. Bunun yanında belediyeler vatandaş bilgisi, imar, vb. satış değeri olan bilgileri tutan kuruluşlar olmaları nedeniyle sıradan siber saldırganlar açısından da iştah açıcı hedeflerdir.

2018 yılında Belediyelere Yapılan Siber Saldırılar

2018 yılı başından itibaren Türkiye'deki belediyelere yapılan siber saldırı sayısı 150'ye yakındır.

Yurtdışında yaşanan bazı örneklere bakacak olursak;

- Ağustos ayında Alaska'da bir belediyenin çalışanları, bilgisayar sistemlerini etkileyen fidye yazılımı nedeniyle bir süre resmi yazışmalar için daktilo kullanmış, fatura ya da makbuzları elle yazmak zorunda kalmıştır.
- Nisan ayında Saint Maarten'in vatandaşa verilen tüm kamu hizmetleri saldırganlarca durdurulmuştur.
- Amerika'da Baltimore, Charlotte, Dallas ve San Francisco belediyeleri benzeri siber saldırıların kurbanı olurken, en büyük zarara uğrayan Atlanta'da tüm şehir sistemlerini bir hafta boyunca etkileyen bir zararlı yazılım kullanılmıştır. The SamSam zararlı yazılım atağı olarak bilinen siber saldırı sonucu 22 Mart 2018'de Atlanta şehrinin tüm bilgisayar sistemi etkilenmiş ve son tahminlere göre 17 milyon dolar civarında hasara neden olmuştur. Atlanta Belediyesi, zararlı yazılım ile şifrelenen dosyaların açılması için saldırganların talep ettiği fidyeyi ödemeyi kabul etmemesine rağmen bu Amerikan tarihinde bir belediyeye yapılan en yüksek maliyetli saldırı olmuştur.
- Eylül ayında ise Kanada'da iki belediye siber suçlulara on binlerce dolar fidye ödemek zorunda kalmıştır. Sunucularında bulunan verilerin şifrelenmesi üzerine bir süre şifreleri kırmaya çalışan belediyeler başarısız olunca çareyi talep edilen fidyeleri ödemekte bulmuştur.

Belediyeleri Hedef Alan Siber Saldırıları Türleri

Siber saldırıların kapsamı ve karmaşıklığı gittikçe artmaktadır. MarketsandMarkets isimli araştırma firmasının verilerine göre siber güvenlik pazarı 2016 yılında 122,45 milyar dolar iken bu rakamın 2021 yılında 202,36 milyar dolara ulaşması, veri sızıntılarından oluşacak maliyetin 2019 yılında 2 trilyon dolar civarında olması beklenmektedir.
Saldırıların ölçek ve kapsamı değişmekle birlikte, yapılan siber saldırılar genellikle aşağıdaki beş kategoriden birine girmektedir:

Ağ ve Uygulama Katmanı Saldırıları

Bu saldırılar en fazla maruz kalınan ve en zor savunma yapılabilenlerdir. İnternet bağlantılı sunucu ve ağ kaynaklarının askıya alınmasıyla sonuçlanır. Saldırıları düzenlemek için gerekli olan istismar kitleri internet üzerinden temin edilebilmekte olduğundan bu saldırıları düzenlemek basit hale gelmektedir. Pek çok çeşidi olmakla birlikte en bilinenleri şunlardır:

- DDos (Denial of Service)
- Kaba Kuvvet (Brute Force) Saldırıları
- SSL (Secure Socket Layer) Saldırıları

Sosyal Mühendislik

Teknik zafiyetlerden ziyade insan duygularından kaynaklanan hatalara dayanan sosyal mühendislik saldırıları, kurbana gönderilen sahte bir e-posta veya farklı iletişim yöntemleri ile kişisel bilgilerin, kullanıcı adı ve parolalarının ele geçirilmesi sonucu ortaya çıkar. Kaynak geçerli gibi görünüyor olduğundan fark edilmesi güçtür. Oltalama saldırıları sosyal mühendislik saldırılarının yaygın bir çeşididir. Kritik bilgilerin saldırganların eline geçmesine neden olabilmektedir.

Gelişmiş Sürekli Tehdit (APT)

"Hedef Odaklı Saldırı" olarak da tanımlanabilir. Kuruluş güvenliğini en çok tehdit eden saldırı türlerinin başında gelmektedir. En gelişmiş teknik beceri ve en yüksek seviyede motivasyon gerektiren saldırılardır.
APT saldırıları özellikle Kamu Kurumlarını, kritik altyapıları, büyük şirketleri, finans sektörünü ve telekom operatörlerini hedef almaktadır.

Siber Suç Örgütleri

Organize siber suçlar gittikçe yaygınlaşmaktadır. McAfee raporuna göre Rusya'da faaliyet gösteren devlet destekli yaklaşık 30 adet siber suç örgütü bulunmaktadır. Siber suç işlenmesi için hizmet veren bu örgütler zararlı yazılım dağıtılmasından kredi kartı bilgilerinin çalınmasına kadar pek çok farklı alanda hizmet vermektedir.

Majör Veri Sızıntıları

Majör veri sızıntısı bir ağa sızılarak çok miktarda hassas verinin elde edilmesi, ifşa edilmesi ya da operasyonları aksatmak amacıyla kullanılması anlamına gelmektedir. 2013 yılından beri Türkiye'de 100 milyondan fazla kişisel verinin çalındığı tahmin edilmektedir. Dünya genelinde ise saniyede 56, dakikada 3338 ve günde 200.263 verinin çalındığı istatistikler tarafınca gösterilmektedir.

Aşağıdaki tablolarda University of Maryland tarafınca Amerika'da yapılan bir anketin sonuçları yer almaktadır.

Belediyelere Yapılan Siber Saldırıların Sıklığı

University of Maryland tarafınca açıklanan rapora göre; araştırmaya katılan belediyelerin 44%'ü günde en az 1 adet siber saldırıya maruz kalmaktadır.

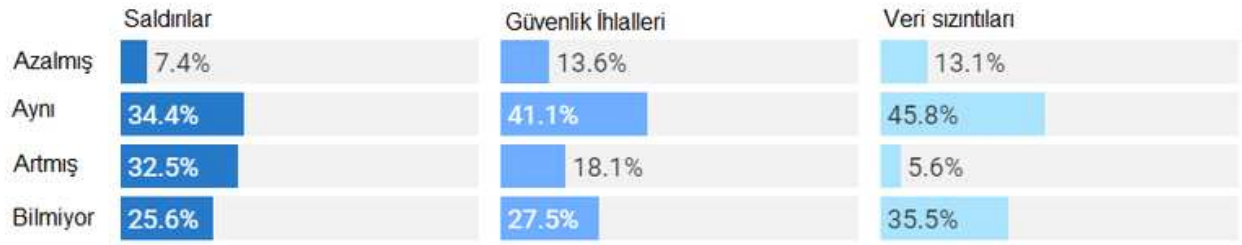
Aşağıdaki tabloda ankete katılan belediyelerin yaşadığı ihlallerin sıklığı görülebilmektedir:

Yerel Yönetimlere yapılan saldırılar

Güvenlik ihlalleri: Bir bilgisayar sisteminin gizliliğini, bütünlüğünü veya kullanılabilirliğini tehlikeye atan olaylardır.
Veri sızıntıları: Bilginin yetkisiz bir kişinin eline geçmesi ile sonuçlanan olaylardır.

Belediyelere Yapılan Siber Saldırılarda Yıllar İçinde Görülen Artış

Aşağıdaki tabloda belediyelerin yaşadığı ihlallerin önceki yıllara oranla artış/azalış durumları görülebilmektedir:



Saldırılar: Zarar vermek için yetkisiz erişim elde etme girişimleridir.
Güvenlik ihlalleri: Bir bilgisayar sisteminin gizliliğini, bütünlüğünü veya kullanılabilirliğini tehlikeye atan olaylardır.
Veri sızıntıları: Bilginin yetkisiz bir kişinin eline geçmesi ile sonuçlanan olaylardır.

Tabloda görüldüğü üzere çok sayıda belediye; saldırı, güvenlik ihlali ya da veri sızıntılarının önceki yıla göre arttığını veya aynı seviyede kaldığını belirtmiştir.

Belediyelerin önemli bir kısmı ise ne sıklıkta saldırıya uğradığını bilmemekte ya da saldırıları kayıt altına almamaktadır.

Muhtemel bir Siber Saldırı Sonucu Oluşabilecek Zararlar

Kritik hizmetlerin durması

Networklerin işlevsiz hale gelmesine neden olabilecek bir zararlı yazılım belediye çalışanlarının ve halkın kritik hizmetlere erişememesine neden olabilir.

Veri kaybı

Saldırı anında kritik verilere erişemez hale gelmenin yanı sıra yaşanmış pek çok olayda mevcut verilerin tamamen kaybedildiğine şahit olunmuştur.

Verimlilik kaybı

Siber saldırılarda yaşanan kayıpların en ağırı hem özel sektör hem kamu hizmetleri açısından verimlilik kaybı olmaktadır. Hizmetlerin aksaması ya da tamamen durması sonucunda yaşanan kayıp fiziki kayıplardan daha büyük zarara neden olmaktadır. E-postalara erişememek, verilen hizmetlerin manuel olarak (kalem kâğıt ile) yapılmak zorunda kalınması, hizmetin tamamen durması gibi sonuçlar doğurabilmektedir. Colorado Belediyesi'ne yapılan saldırıda 2000 çalışanın bilgisayarı bir hafta süreyle çalışamaz hale gelmiş ve bu 80.000 saatlik bir iş gücü kaybına neden olmuştur.

Kurtarma maliyeti

Bütçe planlamaları içerisinde yer almayan beklenmedik maliyetlerin yükü ağır olabilmektedir. A.B.D. Allentown eyaletinde Emotet virüsü sonrası sistemlere yansıyan kurtarma maliyeti yaklaşık 1 milyon USD, 2017 yılında Kansas eyaletinde yaşanan hacklenme olayı sonrası ise 1.2 milyon USD olmuştur. Bu maliyetler operasyon bütçesi içerisinde yer almadığından bahsi geçen belediyeleri zor durumda bırakmıştır.

Belediye gelirlerinin toplanamaması

Siber saldırıların getireceği ek maliyetlerin yanı sıra belediye gelirlerinin zamanında toplanamamasına da etkisi olacaktır. Yapılması gereken ödemelerin zamanında yapılamaması ve alınacak olan ödemelerin alınamaması sonucu (kullanıcıların online ödemelerinin durması vb. gibi durumlarda) oluşabilecek zarar hesaba katılmalıdır.

Vergi mükelleflerinin zararı

Belediyelerde yaşanacak olası bir siber saldırı durumunda yaşanacak zarar yalnız belediye çalışanlarını değil vergi mükelleflerini de direkt olarak etkileyecektir. Zararlı yazılım bulaşması sonucunda etkilenecek sistemler nedeniyle online işlemler yapılamayacak, yaşanacak aşırı yoğunluklar nedeniyle halk etkilenecektir.

Güven kaybı

Özel sektörde olduğu gibi belediyelerin de bir marka imajı vardır ve itibarlarını düşünmesi gerekmektedir. Olası bir siber saldırı sonucunda yaşanabilecek güven kaybı özellikle seçim dönemlerinde seçmen kararını dahi etkileyebilecektir.

Siber Güvenlik Yönetim Stratejisi

Siber güvenlikten doğan risklerin yönetimi konusunda etkili kabul edilen yöntemlerin başında risk odaklı yaklaşım gelmektedir. Bu yaklaşım sayesinde siber tehditlerden doğabilecek riskler denetim altına alınabilir ve siber güvenlik seviyesinin sürekli artırılması mümkün olabilmektedir.

Bu model kapsamında belediyelere önerilerimiz aşağıdakiler olacaktır:

Risk odaklı yaklaşım

Belediyenin siber risk seviyesinin belirlenmesi ve yönetilmesi için bir yöntem belirlenmesi gerekmektedir. Bu yöntemin tutarlı olması belediyenin genel risk seviyesinin tutarlı bir biçimde ortaya konulabilmesi için önemlidir. Belediyenin karşı karşıya olduğu siber risklerin ortaya konulması ve kabul edilebilir risklerin belirlenmesi yönetim modelinin çerçevesinin oluşturulması açısından önemlidir.

Önceliklendirme

Ortaya konulan risklere bağlı olarak siber güvenlik konusunda önceliklerin belirlenmesi yatırım kararlarını ve siber güvenlik yol haritasını bütçe kısıtlarına uygun olarak ve gerçekçi biçimde şekillendirmek için önemlidir. Önceliklendirme konusunda yöneticilerin bilinçlendirilerek ihtiyaç duyulabilecek finans ve personel ihtiyaçlarının doğru anlaşılması ve desteklenmesi sağlanabilir.

Güvenlik kriterlerinin belirlenmesi

%100 güvenlik sağlanmak mümkün olmadığı için belediye açısından siber güvenlik etkinliğinin değerlendirilmesi ve iyileştirilmesi için gerekli belediyenin kendi bünyesinde bulunan sistemlerin güvenlik kriterlerini belirlemesi gerekiyor. Belirlenecek kriterlerin ölçülmesi, iyileştirilmesi ve tekrar ölçülmesinden oluşturulacak bir döngü siber güvenlik seviyesinin sürekli iyileştirilmesine imkân verir. Sunucular, ağ yönetim cihazları, işletim sistemleri, belediye bünyesinde kullanılan uygulamalar, güvenlik yazılımları ve kullanıcı parolaları gibi başlıklar için belirlenecek asgari kriterler ve hedefler iyileştirme sürecini destekler. Bu çerçevede belirlenen kriterlerin belirli aralıklarla ve düzenli olarak izlenmesi için bir süreç oluşturması gerekir.

Bilgi paylaşımı

Belediye sınırları içerisinde bulunan ve/veya belediyeye bağlı kuruluşların (kurum, iştirak, ulaşım hizmeti, vb.) yapılarla siber riskler konusunda bilgi alışverişi yapılması siber saldırıların tespiti ve engellenmesini kolaylaştırır. Bu nedenle bu kuruluşlarla siber saldırılar ve tehditler konusunda bilgi paylaşımı yapılmasına imkân verecek bir yapının oluşturulması gerekir. Bu yapıya dahil kuruluşlarda belirlenecek iletişim noktası (kişi veya birim) belirlenerek bilgi paylaşımının nasıl ve hangi durumlarda yapılacağı belirlenmelidir. Bilgi paylaşımının etkinliğinin ölçülmesi için kurulacak yapının belirli aralıklarla test edilmesi ve bilgi paylaşım süreçlerinin iyileştirilmesi önemlidir.

Olay müdahale becerileri

Belediye bünyesinde kurulacak bir S.O.M.E. (Siber Olaylara Müdahale Ekibi) ile tespit edilecek güvenlik ihlallerine etkin müdahale yapılmalıdır. Bu çerçevede S.O.M.E. ekibine dahil olacak personelin eğitim ihtiyaçlarının karşılanması ve olay tespit ve müdahalesine imkân verecek log yönetimi ve merkezi log yönetimi çözümlerinin tedarik edilmesi gerekecektir.

Farkındalığın artırılması

Siber güvenlik sadece Bilgi İşlem biriminin emeği ve teknolojik yatırımlarla mümkün değildir. Belediye genelinde personelin siber güvenlik konusunda farkındalığının artırılması için eğitim ve test süreçleri işletilmelidir.

Tedarik süreci

Belediyenin vatandaşa hizmet vermek için veya kendi bünyesinde kullandığı teknolojik altyapı ve yazılımların tedarik sürecinden doğabilecek siber güvenlik risklerine karşı etkili bir kontrol mekanizması kurulmalıdır. Bu kapsamda tedarik edilecek veya belediye bünyesine geliştirilen yazılımların kaynak kod analizlerinin yapılması, tedarikçilerin kendi bünyelerinde kullandıkları ağ ve sistemlerin güvenlik seviyelerinin denetlenmesi riskleri azaltacaktır.

Siber Güvenlik Kontrolleri

Belediye bünyesinde bulunması gereken asgari siber güvenlik kontrolleri temel, yapısal ve örgütsel olarak 3 gruba ayrılabilir:

Temel kontroller

İlk aşamada temel siber güvenlik kontrollerinin yapıldığından emin olunmalıdır. Bu kapsamda aşağıdaki süreçlerin oluşturulması ve işletilmesi gerekmektedir.

- Donanım envanterinin çıkartılması
- Yazılım envanterinin çıkartılması
- Sürekli zafiyet denetiminin yapılması
- Kullanıcı yetkilerinin denetlenmesi
- Sistemlerin güvenli kurulumu
- Sistem loglarının izlenmesi

Yapısal kontroller

Temel güvenlik kontrollerinin oluşturulmasının ardından yapısal kontroller ile ikinci bir savunma hattı oluşturulmalıdır. Yapısal güvenlik kontrolleri en az aşağıdaki başlıkları içermelidir;

- E-posta ve internet tarayıcısı güvenlik önlemleri
- Zararlı yazılımlarına karşı tedbirler
- Ağ protokol, port ve servislerin sınırlandırılması
- Veri kurtarma becerilerinin geliştirilmesi
- Firewall, router, vb. ağ cihazların güvenlik ayarlarının yapılması
- Ağ sınır güvenliği için gerekli tedbirlerin alınması
- Veri güvenliğini sağlamaya yönelik tedbirlerin alınması
- Ağ erişim yetkilerinin denetlenmesi
- Kablosuz ağların güvenliğinin sağlanması
- Kullanıcı hesaplarının denetimi ve izlenmesi

Örgütsel kontroller

İlk iki kademenin oluşturacağı güvenlik seviyesinin korunabilmesi ve genel siber güvenlik duruşunun etkinliğinin sağlanması için bu adımlar örgütsel seviyede siber güvenlik tedbirleriyle desteklenmelidir. Bunlar en azından;

- Siber güvenlik farkındalık programının oluşturulması
- Uygulama güvenliğinin sağlanması
- Olay müdahalesi becerileri
- Sızma testleri

olarak düşünülmelidir.

Sparta Bilişim Teknolojileri Yazılım Danışmanlık Sanayi ve Ticaret Ltd. Şti.

Adres: Mustafa Kemal Mahallesi Dumlupınar Bulvarı No: 266 A/82 Çankaya/Ankara

Telefon: 0 312 909 33 02

Web: www.sparta.com.tr