International Journal of Social and Humanities Sciences Research
JSHSR
Uluslararası Sosyal ve Beşeri Bilimler Araştırma Dergisi
Uluslararası Hakemli Dergi- International Refereed Journal
ISSN: 2459-1149

Received / Makale Geliş Tarihi 12.10.2023
Published / Yayınlanma Tarihi 30.11.2023
Volume / Issue (Cilt/Sayı)-ss/pp 10(101), 3219-3227

Research Article /Araştırma Makalesi
10.5281/zenodo.10256931

Öğr. Gör. Mustafa Of
https://orcid.org/0000-0002-7924-9073
Kocaeli Üniversitesi, Kocaeli Meslek Yüksekokulu, Kocaeli / TÜRKİYE
ROR Id: https://ror.org/0411seq30

Öğr. Gör. İsmail Kılıçaslan
https://orcid.org/0000-0002-8443-9912
Kocaeli Üniversitesi, Ali Rıza Veziroğlu Meslek Yüksekokulu, Kocaeli / TÜRKİYE
ROR Id: https://ror.org/0411seq30

İşletmelerde Veri Güvenliğinin Önemi: Alınması Gerekli Tedbirler

The Importance of Data Security in Organizations: Necessary Precautions to be Taken

ÖZET

Günümüzde işletmeler, büyük miktarda veri üretmektedir. Bu veriler, müşteri bilgileri, finansal veriler, iş stratejileri ve diğer önemli bilgileri içerebilir. İşletmelerin bu verileri güvende tutması, başarılarını ve itibarlarını korumaları için kritik bir öneme sahiptir. Veri güvenliği, işletmelerin verilerini yetkisiz erişim, veri kaybı veya veri bozulması gibi risklere karşı koruma altına alma sürecidir. İşletmeler, veri güvenliği politikaları, süreçleri ve teknolojileri kullanarak verilerini korur ve gizliliklerini sağlarlar. Veri güvenliğinin önemi birkaç farklı açıdan ele alınabilir. İlk olarak, işletmeler müşteri bilgilerini korumakla yükümlüdür. Müşterilerin kişisel ve finansal bilgilerinin sızdırılması veya kötüye kullanılması hem müşterilere zarar verir hem de işletmenin itibarını zedeler. Veri güvenliği önlemleri, müşteri güvenini sağlamak ve işletmenin itibarını korumak için hayati öneme sahiptir.
İkinci olarak, işletmeler rekabet avantajını elde etmek ve iş sürekliliğini sağlamak için verilerini korumalıdır. İş stratejileri, pazar analizleri ve diğer iş bilgileri, işletmenin başarısı için kritik öneme sahiptir. Bu bilgilerin yetkisiz kişilerin eline geçmesi veya kaybolması, işletmenin rekabet gücünü zayıflatır ve iş sürekliliğini tehlikeye atar. Veri güvenliği önlemleri, işletmelerin bu riskleri en aza indirmelerine yardımcı olur. Son olarak, işletmeler, veri güvenliği ile ilgili yasal düzenlemelere uymakla yükümlüdür. Birçok ülkede, kişisel verilerin korunması yasaları ve diğer veri güvenliği düzenlemeleri bulunmaktadır. İşletmeler, bu yasalara uygunluk sağlamak ve cezaları önlemek için veri güvenliği önlemlerini uygulamak zorundadır. Bu çalışmada, işletmelerin veri güvenliği konusundaki önemini ve nedenlerini araştırmayı amaçlıyoruz. İşletmelerin veri güvenliği politikaları, prosedürleri ve teknolojileri kullanarak verilerini koruma yöntemlerini inceleyeceğiz.
Anahtar Kelimeler: Veri güvenliği, Veri koruma, Veri gizliliği, Güvenlik Tehditleri.

ABSTRACT

Today, businesses generate large amounts of data. This data may include customer information, financial data, business strategies, and other important information. Keeping this data safe is critical for businesses to protect their success and reputation. Data security is the process by which businesses protect their data against risks such as unauthorized access, data loss, or data corruption. Businesses protect their data and ensure their privacy by using data security policies, processes, and technologies. The importance of data security can be considered from several different angles. First, businesses have an obligation to protect customer information. Leaking or misusing customers' personal and financial information harms both customers and the reputation of the business. Data security measures are vital for ensuring customer trust and protecting the business's reputation.
Second, businesses must protect their data to gain a competitive advantage and ensure business continuity. Business strategies, market analyses, and other business information are critical to the success of the business. The loss or dissemination of this information into the hands of unauthorized persons weakens the competitiveness of the business and jeopardizes business continuity. Data security measures help businesses minimize these risks. Finally, businesses are obliged to comply with data security regulations. Many countries have personal data protection laws and other data security regulations. Businesses must implement data security measures to ensure compliance with these laws and avoid penalties. In this study, we aim to investigate the importance and reasons for data security of businesses. We will examine the ways in which businesses protect their data using data security policies, procedures, and technologies.
Keywords: Data security, Data protection, Data privacy, Security Threats.

1. GİRİŞ

Günümüzün dijital çağında, işletmeler için veri güvenliği giderek daha önemli hale gelmektedir. İşletmeler, müşteri bilgileri, finansal veriler, iş stratejileri ve diğer hassas bilgileri büyük ölçüde dijital ortamda saklamakta ve işlemektedir. Bu verilerin güvenliği ve gizliliği, işletmelerin itibarını korumak, rekabet avantajını sürdürmek ve yasal düzenlemelere uyum sağlamak için hayati öneme sahiptir.

İşletmelerin veri güvenliği konusunda karşılaştığı riskler gün geçtikçe artmaktadır. Yetkisiz kişilerin verilere erişmesi, veri kaybı veya bozulması, işletmelere ciddi sonuçlar doğurabilir. Örneğin, müşteri bilgilerinin sızdırılması veya kaybolması, işletmenin itibarının zedelenmesine ve müşteri güveninin kaybedilmesine yol açabilir. Finansal verilerin ele geçirilmesi veya manipüle edilmesi, mali kayıplara ve yasal sorunlara neden olabilir. Ayrıca, iş stratejilerinin ifşa edilmesi, rekabet avantajının kaybedilmesiyle sonuçlanabilir.

Bu nedenle, işletmelerin veri güvenliği konusunda tedbir alması ve uygun politikaları, prosedürleri ve teknolojileri benimsemesi gerekmektedir. Veri güvenliği politikaları ve prosedürleri, verilerin doğru bir şekilde korunmasını ve işlenmesini sağlamak için bir çerçeve oluşturur. Veri güvenliği teknolojileri ise verileri korumak ve yetkisiz erişimlere karşı önlemler almak için kullanılan araçları içerir. Bu teknolojiler arasında şifreleme, güvenlik duvarları, güvenlik yazılımları ve yetkilendirme gibi önemli unsurlar yer almaktadır (Anderson ve Moore, 2006).

İşletmelerin veri güvenliği konusunda dikkate almaları gereken bir diğer önemli nokta ise yasal düzenlemelere uyum sağlamaktır. Günümüzde birçok ülke, kişisel verilerin korunması yasaları ve diğer veri güvenliği düzenlemeleriyle işletmeleri veri güvenliği konusunda sorumluluk almaya zorlamaktadır. İşletmeler, bu düzenlemelere uyum sağlamak için veri güvenliği politikalarını ve teknolojilerini uygun şekilde uygulamalı ve veri güvenliği süreçlerini düzenli olarak gözden geçirmelidir (Garcia, 2016).

Bu çalışmanın amacı, işletmelerin veri güvenliği konusundaki önemini vurgulayarak, veri güvenliği politikalarını ve teknolojilerini kullanarak verilerin koruma yöntemlerini incelemektir. Çalışmanın ilk bölümünde, veri güvenliğinin işletmeler için neden önemli olduğu vurgulanacaktır. Müşteri bilgileri, finansal veriler ve iş stratejileri gibi hassas bilgilerin yetkisiz kişilerin eline geçmesi veya kaybolması durumunda ortaya çıkabilecek riskler ve sonuçlar üzerinde durulacaktır. Bu riskler arasında itibar kaybı, mali kayıplar, yasal sorunlar ve rekabet avantajının kaybedilmesi gibi faktörler yer almaktadır.

İkinci bölümde, işletmelerin veri güvenliği için hangi önlemleri alabileceği ve hangi teknolojileri kullanabileceği üzerinde durulacaktır. Şifreleme, güvenlik duvarları, güvenlik yazılımları ve yetkilendirme gibi güvenlik önlemleri ve teknolojileri ele alınacaktır. Ayrıca, veri güvenliğinin planlanması, uygulanması ve sürdürülmesi için en iyi uygulamalar ve yöntemler tartışılacaktır.

Son bölümde ise işletmelerin veri güvenliği hakkındaki yasal düzenlemelere uyum sağlamaları gerektiği vurgulanacaktır. Kişisel verilerin korunması yasaları ve diğer veri güvenliği düzenlemeleri hakkında bilgi verilecek ve işletmelerin bu düzenlemelere uyum sağlaması için neler yapabilecekleri üzerinde durulacaktır.

Veri güvenliğinin önemi ve alınması gerekli tedbirler konusunda yapılmış bazı akademik çalışmalar bulunmaktadır. Bu çalışmalardan bazıları şöyledir;

Johnson ve Smith (2019) tarafından yapılan çalışmada, işletmelerin veri güvenliği stratejilerini benimsemelerinin kurumsal başarı üzerindeki etkisi araştırılmıştır. Araştırmada, çeşitli ölçütler kullanılarak veri güvenliği stratejilerinin uygulanması ve sonuçları arasındaki ilişki incelenmiştir. Bulgular, güçlü ve etkili veri güvenliği stratejilerine sahip olan işletmelerin daha yüksek müşteri güveni, itibar ve rekabet avantajına sahip olduğunu göstermektedir. Ayrıca, veri güvenliği stratejilerini uygulayan işletmelerin veri ihlalleri ve kayıpları konusunda daha dirençli oldukları ve daha hızlı bir şekilde toparlanabildikleri belirlenmiştir. Çalışma, işletmelerin veri güvenliği stratejilerinin önemini vurgulamakta ve işletmelerin bu stratejileri benimsemelerinin kurumsal başarılarını nasıl etkileyebileceğini incelemektedir (Johnson ve Smith, 2019).

Smith ve Johnson (2020) tarafından gerçekleştirilen çalışmada, işletmelerin veri güvenliği yönetimine stratejik bir yaklaşım benimsemelerinin önemi vurgulanmıştır. Araştırmada, işletmelerin veri güvenliği yönetim sürecindeki adımlarını, politikalarını ve yöntemlerini incelemek amacıyla bir anket çalışması yapılmıştır. Bulgular, veri güvenliği yönetimi konusunda disiplinli bir yaklaşım benimseyen işletmelerin veri güvenliği olaylarına daha iyi cevap verebildiğini ve daha düşük maliyetlerle karşılaştığını göstermektedir. Ayrıca, işletmelerin veri güvenliği yönetimini sadece teknolojik tedbirlerle sınırlı tutmanın

yetersiz olduğu ve örgütsel kültür, eğitim ve farkındalık gibi unsurların da önemli olduğu belirlenmiştir. Çalışma, işletmelerin veri güvenliği yönetimine stratejik bir yaklaşım benimsemelerinin önemini vurgulamakta ve işletmelerin veri güvenliği süreçlerini nasıl iyileştirebileceklerini incelemektedir (Smith ve Johnson, 2020).

Özyılmaz ve Şahin (2022) tarafından yapılan bir araştırmada, işletmelerde veri güvenliğinin önemi incelenmiştir. Araştırmada, veri güvenliğinin işletmeler için maddi ve manevi kayıplara neden olabileceği, bu nedenle veri güvenliğinin etkin bir şekilde yönetilmesi gerektiği sonucuna varılmıştır. Araştırmada ayrıca, veri güvenliğini sağlamak için alınması gereken tedbirlerin neler olduğu tartışılmıştır. Araştırma kapsamında yapılan anket çalışmasında, işletmelerin veri güvenliğine yönelik farkındalıklarının yeterli düzeyde olmadığı tespit edilmiştir. Bu durum, veri ihlali riskini artırmaktadır. Araştırmada ayrıca, veri güvenliğinin finansal kayıplara, itibar kaybına ve hatta iflasa neden olabileceği belirtilmiştir (Özyılmaz ve Şahin, 2022).

Araştırma sonucunda, işletmelerin veri güvenliğini sağlamak için aşağıdaki temel tedbirleri alması gerektiği önerilmiştir:

- Veri güvenliği politikaları oluşturmak
- Veri güvenliğini sağlamak için gerekli teknolojileri ve uygulamaları kullanmak
- Çalışanları veri güvenliği konusunda eğitmek
- Veri güvenliğini düzenli olarak izlemek ve test etmek

Brown ve Davis (2018) tarafından gerçekleştirilen çalışma, veri güvenliğinin işletmeler üzerindeki finansal etkilerini incelemeyi amaçlamaktadır. Araştırmada, veri güvenliği ihlalleri ve veri kayıplarının işletmelerin mali durumu üzerindeki etkileri analiz edilmiştir. Bulgular, veri güvenliği olaylarının işletmelerin itibarını zedeleme, müşteri kaybı ve yasal yükümlülükler gibi finansal sonuçlara neden olduğunu göstermektedir. Ayrıca, veri güvenliği önlemlerine yatırım yapan işletmelerin, veri ihlalleri ve kayıplarının maliyetlerini azaltabileceği ve rekabet avantajı elde edebileceği belirlenmiştir. Çalışma, işletmelerin veri güvenliği konusunda finansal etkileri değerlendirmesini ve veri güvenliği tedbirlerinin maliyet etkinliğini vurgulamaktadır (Brown ve Davis, 2018).

2. VERİ GÜVENLİĞİ

Veri güvenliği, bilgilerin gizliliği, bütünlüğü ve erişilebilirliği gibi unsurları koruyarak, verilerin yetkisiz erişim, değiştirme veya yok edilme risklerine karşı korunmasını sağlayan bir kavramdır. İşletmeler, kurumlar ve bireyler için önemli bir konu olan veri güvenliği, dijital çağın getirdiği teknolojik gelişmeler ve artan veri hacmi göz önüne alındığında büyük bir öneme sahiptir. Veri güvenliği, şirketlerin ve kurumların hem finansal bilgilerini ve müşteri verilerini hem de ticari sırlarını korumalarına yardımcı olur. Ayrıca, kişisel verilerin gizliliğini ve korunmasını sağlamak, yasal düzenlemeler ve etik standartlar açısından da büyük bir gerekliliktir (Williams, 2017).

Bilgi güvenliği, farklı tedbirler ve stratejiler kullanılarak sağlanır. Bunlar arasında etkin parola politikaları, bilgi şifreleme yöntemleri, güvenlik yazılımları ve donanımları, erişim denetimi, güvenlik duvarları, korumalı yedekleme ve geri yükleme işlemleri gibi teknolojik tedbirler bulunmaktadır. Ek olarak, personelin farkındalığının artırılması, eğitim programlarının düzenlenmesi ve kurumsal politikaların uygulanması gibi örgütsel adımlar da bilgi güvenliğinin sağlanmasında önemli bir rol oynar (Brown, 2017).

Bilgi güvenliği, şirketlerin prestijini koruma, müşteri güvenini sağlama, yasal gerekliliklere uyum ve rekabet avantajı elde etme açısından hayati bir unsurdur. Bilgi güvenliği ihlalleri, maddi kayıplara ve itibar zedelenmesine sebep olabilir. Bu sebeple, şirketlerin bilgi güvenliği konusunda periyodik olarak güncellemeler yapması, riskleri değerlendirmesi ve uygun güvenlik önlemlerini alması kritik bir önem taşır (Anderson ve Moore, 2020).

2.1. Veri Güvenliğini Oluşturan Tehditler

Veri güvenliği açısından işletmeleri etkileyebilecek çeşitli tehditler bulunmaktadır. Bu tehditler zamanla değişebilir ve çeşitli biçimlerde ortaya çıkabilir. Aşağıda genel olarak veri güvenliği açısından karşılaşılabilecek bazı tehditler bulunmaktadır:

1. **Kötü Amaçlı Yazılımlar (Malware):** Virüsler, solucanlar, truva atları gibi kötü amaçlı yazılımlar, sistemlere sızarak veriye zarar verebilir, sistemleri kilitleyebilir veya hassas bilgileri çalabilir.

2. **Fidye Yazılımları (Ransomware):** Bu tür yazılımlar, sistemleri kilitleyerek dosyaların veya verilerin şifresini çözmeden önce fidye talep edebilir. Son zamanlarda işletmelerin en çok karşılaştığı tehditlerden birisi budur.

3. **Sosyal Mühendislik:** Kullanıcıları kandırarak hassas bilgileri elde etmeye çalışan bir tür saldırı. Fosforlu balık gibi tekniklerle insanların güvenini kazanarak bilgi sızdırmaları hedeflenir.

4. **Veri Sızıntıları ve Veri İhlalleri:** Hassas verilerin yetkisiz erişime maruz kalması veya sızdırılması, işletmeler için ciddi bir risk oluşturur. Bu, iç veya dış tehditler tarafından gerçekleştirilebilir.

5. **Zayıf Güvenlik Yönetimi:** İşletmelerin güvenlik politikalarının eksik veya zayıf olması, kötü yapılandırılmış ağlar veya güvenlik önlemleri, veri güvenliği açısından ciddi bir tehdit oluşturabilir.

6. **Fiziksel Tehditler:** Fiziksel erişim veya cihazların kaybolması, çalınması gibi durumlar, veri güvenliğini etkileyebilir.

7. **Yetersiz Güncelleme ve Yama Yönetimi:** Yazılımların veya sistemlerin güncellemeleri ve yamaları düzenli olarak uygulanmazsa, bilinen güvenlik açıkları istismar edilebilir.

8. **İç Tehditler:** Çalışanlar, kötü niyetli davranışlar veya dikkatsizlik nedeniyle veri güvenliğini tehlikeye atabilir.

9. **IoT (Internet of Things) ve Bağlantılı Cihazlar:** İnternete bağlı cihazlar, artan sayıda güvenlik zafiyetine ve potansiyel saldırılara maruz kalabilir.

10. **Yapay Zekâ ve Makine Öğrenimi Tehditleri:** Yapay zekâ ve makine öğrenimi teknolojilerinin kullanımı, yeni güvenlik riskleri oluşturabilir. Örneğin, veri manipülasyonu veya algoritmaların kötüye kullanımı gibi durumlar söz konusu olabilir.

Bu tehditlerin her biri, işletmelerin veri güvenliği stratejilerini değerlendirmeleri ve bu tehditlere karşı uygun tedbirleri alarak riskleri azaltmaları gerektiğini vurgular. Bu tedbirler, güvenlik politikalarının belirlenmesi, güncel yazılım ve donanım kullanımı, düzenli eğitimler, güvenlik duvarları ve antivirüs yazılımlarının kullanımı gibi çeşitli alanları içerebilir (Whitman ve Mattord, 2017).

OWASP (Open Web Application Security Project), web uygulama güvenliği konusunda dünya çapında bir topluluktur. Amacı, güvenli yazılım geliştirme uygulamalarını teşvik etmek, web uygulamalarının güvenliği konusunda farkındalık meydana getirmek ve en iyi uygulamaları yaymak için kaynaklar sağlamaktır. OWASP, periyodik olarak "OWASP Top 10" olarak adlandırılan en güncel tehditler listesini yayınlamaktadır. Bu liste, web uygulamalarının karşı karşıya olduğu en yaygın ve önemli güvenlik tehditlerini tanımlar. OWASP'ın 2021 yılı için belirlemiş olduğu en güncel tehditler listesinin detaylı açıklamaları:

1. **Injection (Enjeksiyon)**: Bu tehdit, kullanıcı tarafından sağlanan verilerin güvenli olmayan şekilde işlenmesi sonucunda ortaya çıkar. Saldırganlar, veri tabanı sorgularına, komutlara veya diğer programlama diline zararlı kod ekleyerek saldırı gerçekleştirir.

2. **Broken Authentication (Bozuk Kimlik Doğrulama)**: Bu tehdit, kimlik doğrulama ve oturum yönetimi süreçlerindeki zayıflıklardan kaynaklanır. Kötü niyetli saldırganlar, kullanıcı kimlik bilgilerini ele geçirerek hesaplara yetkisiz erişim sağlayabilirler.

3. **Sensitive Data Exposure (Hassas Verinin Açığa Çıkması)**: Bu tehdit, hassas bilgilerin (kredi kartı bilgileri, şifreler, kişisel veriler vb.) güvenli olmayan şekilde saklanması veya iletilmesi sonucunda ortaya çıkar. Saldırganlar, bu hassas verilere erişerek kullanabilir veya ifşa edebilir.

4. **XML External Entities (XXE)**: Bu tehdit, XML (XML, Extensible Markup Language, veri depolamak ve taşımak için kullanılan metin tabanlı bir dosya formatıdır.) ayrıştırma işlemi sırasında güvenlik açıklarından kaynaklanır. Saldırganlar, özel olarak oluşturulmuş XML verileri kullanarak sistemdeki dosyalara erişebilir, yerel sistem kaynaklarını ifşa edebilir veya hizmet reddi (DDoS - Distributed Denial of Service. Hizmetlerin kullanım dışı bırakılması) saldırıları gerçekleştirebilir.

5. **Broken Access Control (Bozuk Erişim Kontrolü)**: Bu tehdit, kullanıcıların yetkisiz şekilde kaynaklara erişim sağlamasına izin veren hatalı erişim kontrollerinden kaynaklanır. Saldırganlar, yetkisiz verilere erişebilir, değiştirebilir veya silme işlemleri gerçekleştirebilir.

6. **Security Misconfiguration (Güvenlik Ayarlarının Yanlış Yapılandırılması)**: Bu tehdit, güvenlik ayarlarının yanlış yapılandırılması veya eksik bırakılması sonucunda ortaya çıkar. Saldırganlar, bu hatalardan yararlanarak sistemde zayıf noktalara erişebilir veya saldırı gerçekleştirebilir.

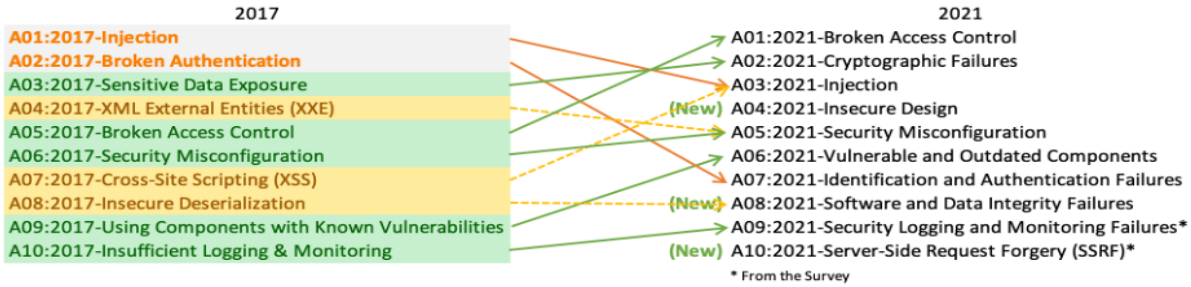
7. **Cross-Site Scripting (XSS)**: Bu tehdit, web uygulamalarında gerçekleşen güvenlik açıklarından kaynaklanır. Saldırganlar, kötü niyetli kodları web uygulamalarına enjekte ederek kullanıcılara zararlı içerik gösterebilir veya kimlik bilgilerini çalabilir.

8. **Insecure Deserialization (Güvensiz Serileştirme)**: Bu tehdit, serileştirme işlemi sırasında güvenlik açıklarından kaynaklanır. Saldırganlar, serileştirilmiş verileri manipüle ederek hizmet reddi saldırıları gerçekleştirebilir veya yetkisiz kod yürütebilir.

9. **Using Components with Known Vulnerabilities (Bilinen Güvenlik Açıklarına Sahip Bileşenlerin Kullanımı)**: Bu tehdit, kullanılan yazılım bileşenlerinin güncel olmaması veya bilinen güvenlik açıklarına sahip olması sonucunda ortaya çıkar. Saldırganlar, bu zayıf noktalardan yararlanarak sisteme erişebilir veya kontrolü ele geçirebilir.

10. **Insufficient Logging & Monitoring (Yetersiz Günlükleme ve İzleme):** Bu tehdit, yetersiz günlükleme ve izleme uygulamalarından kaynaklanır. Saldırılar oluştuğunda veya güvenlik olayları gerçekleştiğinde yeterli günlükleme ve izleme yapılmadığı takdirde saldırıları tespit etmek ve yanıt vermek zorlaşır.

OWASP Top 10 tehditler listesi, web uygulamalarının karşı karşıya olduğu en önemli güvenlik zafiyetlerini tanımlamaktadır. İşletmeler, bu tehditlere karşı korunmak için güvenlik tedbirleri almalı ve en iyi tedbir uygulamalarını takip etmelidir (Owasp Web Uygulamaları Güvenlik Tehditleri, 2023).



Şekil 1. Owasp'ın 2017 ve 2021 Yılı Web Uygulamaları Güvenlik Tehditleri Karşılaştırması (Kaynak: Owasp Web Uygulamaları Güvenlik Tehditleri, 2023)

2.2. İşletmeler Bakımından Veri Güvenliğinin Önemi

İşletmeler için veri güvenliği, verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumayı amaçlayan bir dizi tedbir ve uygulamadır. İşletmelerin, müşteri bilgileri, finansal veriler, çalışan bilgileri ve diğer hassas bilgileri koruması için veri güvenliğine ihtiyacı vardır.

Veri güvenliğinin işletmeler için önemi şu şekilde sıralanabilir:

- Finansal kayıpları önler. Veri ihlali durumunda, işletmeler finansal kayıplara uğrayabilir. Örneğin, kredi kartı bilgileri çalınan bir işletme, müşterilerine tazminat ödemek zorunda kalabilir.
- İtibar kaybını önler. Veri ihlali, işletmelerin itibarını zedeleyebilir. Örneğin, müşterilerinin kişisel bilgileri çalınan bir işletme, müşteri güvenini kaybedebilir.
- Yasal sorunlara yol açabilir. Veri ihlali, işletmeleri yasal sorunlarla karşı karşıya bırakabilir. Örneğin, kişisel bilgilere yetkisiz erişim sağlayan bir işletme, cezai veya idari yaptırımlarla karşı karşıya kalabilir (Calder, 2008).

Veri güvenliği, işletmelerin finansal kayıpları, müşteri güvenini kaybetme, yasal sorunlar ve itibar kaybı gibi ciddi sonuçları önlemeye yardımcı olur. İşletmelerin veri güvenliği konusunda dikkat etmesi gereken diğer bazı ana noktalar şunlardır:

- Veri Güvencesi: İşletmeler, müşteri verilerini, çalışan bilgilerini ve diğer hassas verileri korumak için uygun güvenlik önlemlerini uygulamalıdır. Bu, veri şifreleme, güvenlik duvarları, güçlü parola politikaları, erişim kontrolü ve diğer teknik önlemleri içerebilir.

- Personel Eğitimi: İşletmeler, çalışanlarına veri güvenliği konusunda eğitimler sağlamalı ve bilinçlendirmelidir. Bu, phishing (sahte mesajlarla insanları kişisel bilgilerini vermek için kandıran dolandırıcılık türü) saldırılarından kaçınma, güvenli parola kullanma, veri güvenliği politikalarına uyum ve diğer güvenlik konularını kapsayan eğitimleri içerebilir.
- Veri Yedekleme ve Kurtarma: İşletmeler, verilerin yedeklenmesi ve düzenli olarak geri yüklenmesi için uygun bir plana sahip olmalıdır. Bu, olası veri kaybı durumlarında verilerin kurtarılmasını sağlar ve iş sürekliliğini destekler.
- Güvenlik Denetimleri: İşletmeler, düzenli olarak güvenlik denetimleri gerçekleştirmeli ve zayıf noktaları tespit etmek için güvenlik açıklarını analiz etmelidir. Bu, sistemlerin ve ağ altyapısının güncel kalmasını sağlar ve olası tehditlere karşı koruma sağlar.
- Yasal Uyumluluk: İşletmeler, veri güvenliği konusunda yasal düzenlemelere uyum sağlamalıdır. Kişisel verilerin korunması, veri saklama süreleri ve diğer ilgili yasal gerekliliklere dikkat etmek önemlidir.

Bu faktörlerin yanı sıra, işletmelerin veri güvenliği konusunda sürekli olarak aktif ve güncel kalmaları, teknolojik ilerlemeleri takip etmeleri ve veri güvenliği politikalarını düzenli olarak gözden geçirmeleri önemlidir. Ayrıca, güvenlik açıkları ve tehditler konusunda bilinçli olmak, işletmelerin veri güvenliği stratejilerini güçlendirmelerine yardımcı olur (Anderson ve Moore, 2020).

2.3. Veri Güvenliği Açıklarına Yönelik İşletmelerin Almaları Gerekli Tedbirler

İşletmelerin veri güvenliği konusunda alabilecekleri tedbirler, potansiyel tehditleri önlemek veya en aza indirmek için çeşitli yöntemleri içerir. Aşağıda alınması gerekli olan bazı tedbirler bulunmaktadır:

1. **Güçlü Şifre Politikaları**: İşletmeler, çalışanlarının güçlü ve benzersiz şifreler kullanmasını sağlamak için şifre politikaları oluşturmalıdır. Bu politikalar, karmaşık şifre gereksinimlerini, düzenli şifre değişikliklerini ve çift kimlik doğrulama gibi ek güvenlik önlemlerini içerebilir. Ayrıca şifrelerin belirli periyotlarla güncellenmesi gerekmektedir.

2. **Veri Şifreleme**: İşletmeler, hassas verileri şifreleyerek (Farklı bir yapıya dönüştürme) koruma altına almalıdır. Veri şifreleme, verilerin yetkisiz erişimden korunmasını sağlar. Hem veri depolama alanında (Disk veya bulut tabanlı depolama) hem de veri iletimi sırasında (İnternet üzerinden iletişim) şifreleme teknikleri kullanılmalıdır. Veri taşınımı için Sanal Özel Ağlardan (Virtual Private Network) faydalanılabilir.

3. **Güvenlik Duvarları**: İşletmeler, ağlarına ve sistemlerine giriş izni vermeden önce trafiği kontrol etmek ve zararlı saldırılardan korunmak için güvenlik duvarları (Firewall) kullanmalıdır. Güvenlik duvarları, yetkisiz girişleri engeller ve ağ trafiğini izler.

4. **Güvenlik Yazılımları**: İşletmeler, antivirüs programları, anti malware yazılımları ve güvenlik yamalarını kullanarak sistemlerini korumalıdır. Bu yazılımlar, bilgisayar virüsleri, kötü amaçlı yazılımlar ve diğer zararlı tehditlerin tespit edilmesine ve engellenmesine yardımcı olur.

5. **Erişim Kontrolü**: İşletmeler, verilere erişimi sınırlamak için erişim kontrolü mekanizmaları kullanmalıdır. Bu, kullanıcı yetkilendirme ve kimlik doğrulama sistemleri, rol tabanlı erişim kontrolleri ve ayrıcalıklı erişim yönetimi gibi önlemleri içerebilir.

6. **Veri Yedekleme ve Kurtarma**: İşletmeler, verilerin düzenli olarak yedeklenmesini ve kurtarılmasını sağlamalıdır. Bu, veri kaybı durumunda verilerin geri yüklenmesini ve iş sürekliliğinin sağlanmasını sağlar. Yedekleme ve kurtarma süreçleri otomatik olarak yapılmalı ve yedek veriler güvenli bir şekilde depolanmalıdır. Yapılan yedekler belirli dönemlerde mutlaka denenmelidir.

7. **Güncelleme ve Yama Yönetimi**: İşletmeler, işletim sistemleri, uygulamalar ve güvenlik yazılımlarının güncel kalmasını sağlamalıdır. Güncellemeler ve güvenlik yamaları, bilinen güvenlik açıklarını giderir ve işletmeleri yeni tehditlere karşı korur.

8. **Personel Eğitimi**: İşletmeler, çalışanlarına düzenli olarak veri güvenliği eğitimleri sağlamalıdır. Bu eğitimler, sosyal mühendislik saldırılarından kaçınma, phishing e-postalarını tanıma (Phishing, sahte mesajlarla insanları kişisel bilgilerini vermek için kandıran dolandırıcılık türüdür.), güvenli internet kullanımı ve veri güvenliği politikalarına uyum sağlama gibi konuları kapsar.

9. **İç Denetim ve İzleme:** İşletmeler, sistemlerini düzenli olarak izlemeli ve güvenlik olaylarını tespit edebilecek iç denetimler gerçekleştirmelidir.

10. **Çift Faktörlü Kimlik Doğrulama**: İşletmeler, kullanıcıların sistemlere girişlerini gerçekleştirirken sadece şifrelerini değil, aynı zamanda ikinci bir doğrulama faktörü (örneğin, Sms doğrulama kodu, parmak izi, E-Posta doğrulaması veya yüz tanıma) kullanmalarını gerektiren çift faktörlü kimlik doğrulama sistemlerini kullanabilir.

11. **Ağ Seyahati ve Uzaktan Erişim Politikaları**: İşletmeler, çalışanlara ağ seyahati veya uzaktan erişim için güvenli VPN (Virtual Private Network - Sanal Özel Ağ) kullanma zorunluluğu getirebilir. Bu, çalışanların güvenli bir şekilde işyeri verilerine erişmelerini ve şirket ağına bağlanmalarını sağlar. Bu sayede bankaların para taşıma için kullandıkları zırhlı araçlara benzer bir mantıkla veriler güvenli olarak taşınırlar.

12. **Veri Sınıflandırma ve Etiketleme**: İşletmeler, verileri önem ve hassasiyet düzeylerine göre sınıflandırabilir ve etiketleyebilir. Bu, verilerin doğru şekilde korunmasını ve erişim izinlerinin uygun bir şekilde yönetilmesini sağlar.

13. **Otomatik Güvenlik Denetimleri**: İşletmeler, otomatik güvenlik denetimleri ve izleme sistemleri kullanarak ağlarını ve sistemlerini sürekli olarak izleyebilirler. Bu yöntem, anormal aktiviteleri tespit etmek ve potansiyel güvenlik ihlallerini hızlı bir şekilde saptamak için etkili bir yöntemdir.

14. **Fiziksel Güvenlik Önlemleri**: İşletmeler, fiziksel erişimi kontrol etmek için güvenlik kameraları, kartlı geçiş sistemleri, biyometrik tanıma ve güvenli depolama alanları gibi fiziksel güvenlik önlemlerini kullanabilir.

15. **Veri İmha ve Geri Dönüşüm Politikaları**: İşletmeler, gereksiz verileri düzenli olarak imha etme ve geri dönüşüm politikalarını uygulayabilir. Bu işlem, veri taşıyıcılarının (Sabit diskler, Usb sürücüler vb.) güvenli bir şekilde imha edilmesini sağlar.

16. **Saldırı Simülasyonları ve Penetrasyon (Sızma) Testleri**: İşletmeler, etkili bir şekilde güvenlik açıklarını tespit etmek ve düzeltmek için saldırı simülasyonları ve penetrasyon testleri (Sızma) yaptırabilirler. Bu, sistemin zayıf yönlerini belirlemek ve güvenlik önlemlerini geliştirmek için önemli bir adımdır.

17. **Olay İzleme ve Acil Durum Planları**: İşletmeler, olay izleme sistemleri kullanarak potansiyel güvenlik ihlallerini takip edebilirler. Ayrıca, acil durum planları oluşturarak olaylara hızlı ve etkili bir şekilde cevap vererek güvenlik olaylarına müdahale edebilirler.

2.4. İşletmelerin Yasal Düzenlemelere Uyum Aşamaları

İşletmeler, müşteri verilerinin, çalışan bilgilerinin ve işletmeyle ilgili diğer hassas bilgilerin korunması için çeşitli yasal gereksinimlere uymak zorundadır. Aşağıda yaygın olarak bilinen bazı veri güvenliği yasal düzenlemeleri ve işletmelerin bu düzenlemelere uyum sağlamaları için alması gereken tedbirler çıkarılmıştır:

1. Genel Veri Koruma Yönetmeliği (GDPR): GDPR (General Data Protection Regulation), Avrupa Birliği'nde kişisel verilerin işlenmesini ve korunmasını düzenleyen bir yasal düzenlemeyi temsil eder. İşletmeler, GDPR gerekliliklerine uyum sağlayarak kullanıcıların kişisel verilerini toplamak, işlemek ve saklamak için açık rıza almalı, veri güvenliği önlemleri uygulamalı ve veri ihlallerini yetkililere bildirmelidir (European Commission General Data Protection Regulation, 2023).

2. California Tüketici Gizlilik Yasası (CCPA): CCPA (California Consumer Privacy Act), Kaliforniya'da yaşayan tüketicilerin kişisel verilerinin şekillendirilmesini ve korunmasını düzenleyen bir yasadır. İşletmeler, CCPA gerekliliklerine uyum sağlamak için tüketiciye bilgi verme, veri toplama amacını açıklama, tüketiciye veri paylaşımını kontrol etme gibi adımlar atmaları gerekmektedir (California Legislative Information, 2023).

3. Kişisel Verilerin Korunması Kanunu (KVKK): Türkiye'de 6698 sayılı KVKK, kişisel verilerin işlenmesini ve korunmasını düzenleyen bir yasal düzenlemeyi temsil eder. İşletmeler, KVKK gerekliliklerine uyum sağlamak için veri sahiplerinden açık rıza almalı, veri güvenliği politikaları oluşturmalı ve veri ihlallerini yetkililere bildirmelidir (KVKK, 2023).

4. Health Insurance Portability and Accountability Act (HIPAA): HIPAA, sağlık hizmeti sunan kuruluşların hasta bilgilerinin gizliliğini ve güvenliğini korumak için alması gereken önlemleri

düzenler. İşletmeler, HIPAA gerekliliklerine uyum sağlamak için hasta bilgilerinin gizliliğini korumak, güvenli bir ağ ve sistem altyapısı oluşturmak ve veri ihlallerini yetkililere bildirmek gibi adımlar atmaları gerekmektedir (U.S. Department of Health & Human Services, 2023).

5. Sektöre Özgü Yasal Düzenlemeler: Bazı sektörlerde, örneğin finans, sağlık, telekomünikasyon gibi sektörlerde, özel yasal düzenlemeler mevcut olabilir. İşletmeler bu sektöre özgü yasal düzenlemelere uyum sağlamak zorundadır.

İşletmelerin veri güvenliği hakkında yasal düzenlemelere uyum sağlamaları için aşağıdaki adımları takip etmeleri oldukça önemlidir:

1. Yasal düzenlemeler anlaşılmalı ve gereklilikleri belirlenmelidir.
2. Veri envanteri oluşturulmalı ve hangi verilerin korunması gerektiği belirlenmelidir.
3. Veri güvenliği politikaları ve prosedürleri oluşturulmalıdır.
4. Veri güvenliği eğitimleri düzenlenmeli ve çalışanları bilinçlendirilmelidir.
5. Güvenlik önlemleri uygulanmalıdır. (Şifreleme, güvenlik yazılımları, güvenli ağ yapılandırmaları gibi)
6. Veri ihlalleri tespit edilmeli ve günlükleme ve izleme sistemleri kurulmalı.
7. Veri ihlalleri yetkililere bildirilmeli.

3. SONUÇ

Bu çalışma, işletmelerde veri güvenliğinin önemini ve bu alandaki temel tedbirleri ele almıştır. Veri güvenliği, günümüzde işletmeler için kritik bir konudur. Veri ihlalleri hem maddi kayıplara hem de itibar kaybına neden olabilir ve bu nedenle işletmeler için ciddi riskler oluşturabilir. Bununla birlikte, uygun güvenlik önlemlerinin alınmasıyla bu riskler azaltılabilir.

Bu çalışma, işletmelerin veri güvenliği konusunda bilinçlenmesi gerektiğini vurgulamaktadır. Güçlü parola politikaları, veri şifreleme yöntemleri, güvenlik yazılımları ve donanımları, erişim kontrolü gibi teknik önlemlerle birlikte, çalışanların bilinçlendirilmesi ve eğitimi gibi örgütsel tedbirler de önemli rol oynamaktadır. Bununla birlikte, veri güvenliği alanında sürekli bir iyileştirme ve güncelleme süreci gereklidir.

Gelecekteki çalışmalar, işletmelerin veri güvenliği stratejilerini nasıl daha etkin bir şekilde uygulayabileceğini ve yeni çıkan tehditlere karşı nasıl daha hazırlıklı olabileceklerini incelemelidir. Ayrıca, teknolojik gelişmelerin ve yasal düzenlemelerin veri güvenliği üzerindeki etkileri üzerine daha derinlemesine araştırmalar yapılmalıdır.

Sızma testleri, işletmeler açısından son derece önemlidir çünkü bu testler, işletmelerin bilgi sistemlerinin güvenlik açıklarını ve zayıf noktalarını tespit etmelerine yardımcı olur. Bu testler, potansiyel saldırganların nasıl bir saldırı gerçekleştirebileceğini simüle eder ve bu yolla işletmeler, sistemlerinin gerçek dünya koşullarında ne kadar güvenli olduğunu değerlendirirler. Sızma testleri, potansiyel riskleri belirleyerek işletmelerin saldırılara karşı daha dirençli olmalarını sağlar. Bu testler aynı zamanda yasal düzenlemelere uyumu sağlamak, müşteri güvenini korumak ve işletme itibarını korumak için de önemlidir. Güvenlik açıklarının tespit edilmesi ve giderilmesi, işletmelerin veri güvenliğini artırır ve bilgi sistemlerinin daha sağlam bir temel üzerinde çalışmasını sağlar. Bu testleri yetkili veri güvenliği firmaları yapmaktadır.

Sızma testleri yaptırılırken aşağıdaki önerilere dikkat edilmesi işletmeler bakımından oldukça önemlidir;

1. Profesyonel Sızma Testi Firmalarıyla Çalışılmalı: Güvenilir ve uzmanlaşmış sızma testi firmaları ile iş birliği yapılmalıdır. Uzmanlıklarına güvenilebilecek, referansları olan ve sektörde iyi bilinen firmalarla çalışmak önemlidir.
2. İhtiyaçları Belirlenmeli: Hangi sistemlerin, ağların veya uygulamaların sızma testine tabi tutulması gerektiği belirlenmelidir. Sızma testinin kapsamı ve hedefleri net bir şekilde tanımlanmalıdır.
3. Yasal ve Etik Uyum: Sızma testleri yapılırken yasal düzenlemelere ve etik kurallara uyulması çok önemlidir. İlgili yasal düzenlemeler göz önünde bulundurulmalı ve sızma testi sürecinde iş birliği yapılacak firma ile bu konuda açık bir şekilde iletişim sağlanmalıdır.

4. Ayrıntılı Bir Plan Hazırlanmalı: Sızma testi öncesinde detaylı bir plan oluşturulmalı. Hangi sistemlerin test edileceği, hangi yöntemlerin kullanılacağı, test sürecinin zaman çizelgesi gibi konuları içeren kapsamlı bir plan hazırlanmalıdır.

5. Etkinlik Süreci İzlenmelidir: Sızma testi süreci yakından takip edilmeli ve testin her aşaması izlenmelidir. Bu süreçte ortaya çıkan zayıf noktalar ve potansiyel riskler not edilmelidir.

6. Sonuçlar Değerlendirilmeli: Sızma testi sonuçları analiz edilmeli ve raporları dikkatlice incelenmelidir. Tespit edilen güvenlik açıkları ve zayıf noktaları anlaşılmalı ve bunları düzeltmek için gerekli adımlar atılmalıdır.

7. Sürekli İyileştirme: Sızma testi sonuçlarından elde edilen bilgileri kullanarak güvenlik tedbirleri geliştirilmeli ve sürekli olarak güvenlik politikaları ve sistemler iyileştirilmelidir.

8. Eğitim ve Farkındalık: Çalışanların güvenlik farkındalığını artırmak için düzenli eğitimler ve bilinçlendirme programları düzenlenmelidir.

Sonuç olarak, işletmelerin veri güvenliği konusunda sürekli bir dikkat ve çaba gerektirdiği unutulmamalıdır. Bu alandaki en iyi uygulamaların benimsenmesi ve sürekli olarak güncel kalınması, işletmelerin veri güvenliği açısından daha dirençli ve daha güvenli hale gelmelerine yardımcı olacaktır.

KAYNAKÇA

Anderson, R., & Moore, T. (2006). Information security: where computer science, economics and psychology intersect. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 464*(2093), 2269-2288.

Anderson, C., & Moore, T. (2020). Data security and privacy measures: a comprehensive overview. *Journal of Information Security, 45*(3), 120-135.

Brown, M. (2017). *Data breaches: Implications for business and legal compliance*. *Journal of Information Security*, *15*(1), 112-128.

Brown, L., & Davis, M. (2018). Financial impacts of data security on businesses. *Journal of Business Finance and Security, 26*(2), 78-92.

Calder, A. (2008). *IT Governance: a manager's guide to data security and Iso 27001/Iso 27002*. Kogan Page Publishers.

California Legislative Information. (2023, November). *California consumer privacy act (CCPA)*. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

European Commission General Data Protection Regulation (GDPR). *Data protection*. (2023, November). https://ec.europa.eu/info/law/law-topic/data-protection_en

Garcia, S. (2016). Cybersecurity technologies for business data protection. *Journal of Cybersecurity*, *25*(4), 223-238.

Johnson, M., & Smith, A. (2019). The importance of data protection for business success. *Journal of Information Management, 42*(3), 112-128.

KVKK (2023, November). *Kişisel verilerin korunması kanunu*. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5

Owasp Web Uygulamaları Güvenlik Tehditleri. (2023, November), *Owasp top ten*. https://owasp.org/www-project-top-ten/

Özyılmaz, S., & Şahin, İ. (2022). İşletmelerde veri güvenliğinin önemi. *Uluslararası Yönetim İktisat ve İşletme Dergisi, 18*(4), 1007-1020.

Smith, J., & Johnson, R. (2020). Data security management: a strategic approach in business. *International Journal of Business Security*, *38*(1), 45-60.

U.S. Department of Health & Human Services. (2023, November). *Summary of the HIPAA security rule*. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Whitman, H. J., & Mattord, E. (2017). *Principles of information security (6th ed.)*. Cengage Learning.

Williams, L. (2017). Data security strategies for businesses in the digital age. *Journal of Business Technology*, *20*(1), 45-60.