

**Proaktif Sızma Testi**

**Bilgi Formu**

**İçindekiler**

[Penetrasyon Testi Bilgi Formu 3](#_Toc57123672)

[Dış Test (Black Box) 4](#_Toc57123673)

[İç Test (White Box) 5](#_Toc57123674)

[Web Uygulama Güvenlik Testi 6](#_Toc57123675)

[Mobil Uygulama Güvenlik Testi 6](#_Toc57123676)

[Kablosuz Ağ Güvenlik Testi 7](#_Toc57123677)

[Servis Engelleme (DoS/DDoS) Testi 7](#_Toc57123678)

[Sosyal Mühendislik ve Son Kullanıcı Farkındalık Testi 7](#_Toc57123679)

[Endüstriyel Kontrol Sistemleri (EKS/SCADA) Test Hizmeti 8](#_Toc57123680)

[Kaynak Kod Analizi 8](#_Toc57123681)

[Testler Sırasında Uygulanacak Metodoloji 9](#_Toc57123682)

[Bilgi Toplama Fazı 9](#_Toc57123683)

[Network Haritalama 9](#_Toc57123684)

[Enumerating Fazı 9](#_Toc57123685)

[Zafiyet Tespiti Fazı 10](#_Toc57123686)

[Exploitation Fazı 10](#_Toc57123687)

[Hak Yükseltme Fazı 10](#_Toc57123688)

[Web Uygulama Güvenlik Testleri 11](#_Toc57123689)

[İstemci Tarafı Sızma Testleri 12](#_Toc57123690)

[Servis Dışı Bırakma Testleri 12](#_Toc57123691)

[Veritabanı Zafiyet Testleri 13](#_Toc57123692)

[Kablosuz Ağ Sızma Testleri 13](#_Toc57123693)

[Raporlama 13](#_Toc57123694)

[Sunum 13](#_Toc57123695)

#

# Penetrasyon Testi Bilgi Formu

Penetrasyon testi, zafiyet analizinden farklı olarak belirli bir amaç ve/ veya bir senaryo dahilinde gerçekleştirilmektedir.

Sahip olunan bilişim sistemlerine ait her türlü zafiyetin dış kaynaklı bir kurum ve/veya bir şirket tarafından teste tabi tutulması, kontrol edilmesi ve raporlanması proaktif güvenliğin ilk adımlarındandır. Dış kaynaklı testler şirketlerin farkında olmadıkları her türlü güvenlik açığına farklı bir bakış ile yaklaşarak ve daha koordineli çalışarak bu zafiyetleri ifşa etmek için bir çalışma gerçekleştirirler.

Lütfen gerçekleştirilmesini talep ettiğiniz hizmet türü için kutucuklar içerisine « X » yazınız.

|  |
| --- |
| Penetrasyon Testi İçin Talep Edilen Hizmetler |
| [ ]  Dış Test (Black Box) [ ]  İç Test (White Box) [ ]  Web Uygulama Güvenlik Testi [ ]  Mobil Uygulama Güvenlik Testi [ ]  Kablosuz Ağ Güvenlik Testi [ ]  Servis Engelleme (DOS/DDOS) Testi [ ]  Sosyal Mühendislik ve Son Kullanici Farkındalik Testi [ ]  Endüstriyel Kontrol Sistemleri (EKS/SCADA) Test Hizmeti [ ]  Kaynak Kod Analizi  |

##

## Dış Test (Black Box)

Dış test olarak adlandırılan bu test hedef networke dışarıdan gelecek olan saldırıları simüle edilir. Bu bağlamda bilgileri çalmak, bilgileri yok etmek, bilgiye erişimi yok etmek gibi saldırı türleri simüle edilir. Bu test hackerların yaptığı gerçek saldırılar göz önünde bulundurarak, verecebilecekleri zararları tespit ederek raporlar.

|  |
| --- |
| **Dış Test (Black Box)** |
| **Test Edilecek IP Sayısı (Adet Olarak)**  |  |
| **Test Edilecek Domain (Alan Adı) Sayısı [Sub Domain (Alt Alan Adı) ile birlikte]** |  |
| **DMZ Alanında Bulunan Sunucu Sayısı**  |  |
| **Test Edilecek Sunucu Bilgileri**  | Web Sunucu: | DNS Sunucu:  | Firewall/VPN:  |
| Mail Sunucu:  | FTP Sunucu:  | Diğer:  |
| **Mail Sunucusunun Lokasyonu**  | [ ]  Yerel Lokasyon  | [ ]  Datacenter  |  |
| **Web Sunucusunun Lokasyonu**  | [ ]  Yerel Lokasyon  | [ ]  Datacenter  |  |
| **Sosyal Mühendislik Testi ile Birlikte mi Gerçekleştirilecek**  | [ ]  Evet | [ ]  Hayır |  |

## İç Test (White Box)

İç test olarak da bilinen bu test, gerçekleştirecek firma tarafından müşteri networkünün içerisinde belirli bilgilerin sağlanması yoluyla, içeriden yapılacak saldırıları simüle etme amacıyla gerçekleştirilir. Şirket çalışanlarının ve/veya ağa dahil olan bir saldırganın vereceği zararlar tespit edilerek raporlanır.

|  |
| --- |
| **İç Test (White Box)** |
| **Test Edilecek Toplam Sunucu Sayısı (Fiziksel + Sanal Sunucu)**  | \_\_\_\_ Adet |
| **Client Sayısı**  | \_\_\_\_Adet |
| **Kablosuz Ağ Güvenliği**  | [ ]  Evet | [ ]  Hayır |
| **Kullanılan Veritabanı Sistemleri**  | [ ]  Oracle | [ ]  MS-SQL | [ ]  MySQL | [ ]  Diğer |
| **Çalışma Lokasyonu**  | [ ]  Şirket Merkezi | [ ]  Şehir Dışı Lokasyon |
| **Lokasyon Sayısı**  |  |
| **Lokasyon Adresi - 1**  |  |
| **Lokasyon Adresi - 2** |  |
| **Lokasyon Adresi - 3**  |  |
| **Lokasyon Adresi - 4**  |  |

## Web Uygulama Güvenlik Testi

Web Uygulama Güveblik Testi hedef web uygulamasına gelebilecek olan saldırıları simüle eder. Bu test hackerların yaptığı gerçek saldırıları göz önünde bulundurarak, verecebilecekleri zararları tespit ederek raporlar.

|  |
| --- |
| **Web Uygulama Güvenlik Testi** |
| **Sunucu Sayısı**  |  |
| **Web Uygulama Sayısı**  |  |
| **Teknoloji**  | [ ]  .Net | [ ]  PHP | [ ]  Java |
| **Demo Hesap Sağlanacak mı?**  | [ ]  Evet | [ ]  Hayır |
| **Kullanıcı Profil Sayısı**  |  |

## Mobil Uygulama Güvenlik Testi

Mobil Uygulama Güvenlik Testi hedef mobil uygulamasına gelebilecek olan saldırıları simüle eder. Bu test hackerların yaptığı gerçek saldırıları göz önünde bulundurarak, verecebilecekleri zararları tespit ederek raporlar.

|  |
| --- |
| **Mobil Uygulama Güvenlik Testi** |
| **Mobil Uygulama Sayısı**  |  |
| **Platform**  | [ ]  Android | [ ]  iOS | [ ]  Windows Phone |
| **Demo Hesap Sağlanacak mı?**  | [ ]  Evet | [ ]  Hayır |
| **Erişim adresi (App Store, Google Play Store, vb.)**  |  |
| **Uygulama Ekran Sayısı**  |  |
| **Kullanıcı Profil Sayısı**  |  |

## Kablosuz Ağ Güvenlik Testi

Kablosuz ağ güvenlik testi kablosuz ağların, erişim kontrollerinin, yapılandırmalarının ve kullanıcılarının davranışlarının değerlendirilmesi, parola kırma testleri, erişim sağlanan kablosuz ağlar üzerinden kurum ağına gerçekleştirilebilecek saldırıların test edilmesi, bulgu/çözüm önerilerinin raporlanması ve hizmet kapsamı dahilinde talep edildiğinde doğrulanması faaliyetlerini içeren güvenlik testlerinin gerçekleştirilmesidir.

|  |
| --- |
| **Kablosuz Ağ Güvenlik Testi** |
| **Test Edilecek SSID Sayısı**  |  |
| **Test Yapılacak Lokasyon Sayısı**  |  |

## Servis Engelleme (DoS/DDoS) Testi

Bu testte hedef sisteme yönelik dışardan gelebilecek olan servis dışı bırakma saldırıları belirli bir süre dahilinde simüle edilir.

|  |
| --- |
| **Servis Engelleme (DOS/DDOS) Testi** |
| IP Sayısı |  |
| Sunucu Sayısı |  |
| Bandwith Genişliği | \_\_\_\_\_\_\_ Mbit |

## Sosyal Mühendislik ve Son Kullanıcı Farkındalık Testi

Bu test "Güvenlik zincirindeki en zayıf halka"nın bulunması ve burdan sistemlere sızabilmeyi simüle eder. Sosyal Mühendislik testinde internet üzerinden firma çalışanlarının e-posta hesapları tespit edilmeye çalışılır. Kapsam dahilinde zayıf şifre testleri de gerçekleştirilmektedir.

|  |
| --- |
| **Sosyal Mühendislik ve Son Kullanıcı Farkındalık Testi** |
| **E-posta Gönderilecek Kullanıcı Sayısı**  |  |
| **Varsa, talep edilen senaryolar ve ilave bilgi**  |  |

## Endüstriyel Kontrol Sistemleri (EKS/SCADA) Test Hizmeti

Kurumların Endüstriyel Kontrol Sistemlerinde (EKS) bulunan kapsam dahilindeki EKS ve bilgi sistem bileşenlerinin; zafiyetlerinin tespiti, manuel yöntemlerle denenmesi, analiz edilmesi, bulgu/çözüm önerilerinin raporlanması ve hizmet kapsamında talep edildiğinde doğrulanması faaliyetlerini de içeren güvenlik testleri gerçekleştirilmektedir.

|  |
| --- |
| **Endüstriyel Kontrol Sistemleri (EKS/SCADA) Testi** |
| Test ortamı mevcut mu?  | [ ]  Evet | [ ]  Hayır |
| Üretimdeki sistemler üzerinde de test yapılması isteniyor mu?  | [ ]  Evet | [ ]  Hayır |
| Test kapsamında değerlendirilecek sunucu sayısı?  | ­­­\_\_\_\_Adet |
| Test kapsamında değerlendirilecek uygulama sayısı?  | \_\_\_\_Adet |
| Test kapsamında değerlendirilecek Workstation sayısı?  | \_\_\_\_Adet |
| EKS sisteminde kaç farklı tipte RTU kullanılmaktadır?  | \_\_\_\_ farklı RTU kullanılmaktadır |
| EKS sisteminde kaç farklı tipte PLC kullanılmaktadır?  | \_\_\_\_ farklı PLC kullanılmaktadır |
| EKS sisteminde kaç farklı tipte Röle kullanılmaktadır?  | \_\_\_\_ farklı Röle kullanılmaktadır |
| Test kapsamında değerlendirilecek Router sayısı?  | \_\_\_\_ Adet |
| EKS sisteminde kablosuz ağ teknolojileri kullanılmakta mıdır?  | [ ]  Evet | [ ]  Hayır |

## Kaynak Kod Analizi

Çalışan uygulamaların güvenliği de önemli bir faktördür. Bazı uygulamalar geliştirildikten sonra kod yapısı üzerinde daha sonradan ortaya çıkabilecek zafiyetler sebebi ile güvenlik riski oluşturmuş olabilir. Bu test ile uygulamaların kaynak kodları incelenerek uygulama zafiyetleri ortaya çıkartılarak raporlanır.

|  |  |
| --- | --- |
| Kaynak Kod Analizi |  |
| Sayfa Sayısı | \_\_\_\_ Adet |
| Satır Sayısı | \_\_\_\_ Adet |
| Uygulama Dili | [ ]  C# | [ ]  VB | [ ]  Java | [ ]  PHP |

# Testler Sırasında Uygulanacak Metodoloji

Gerçekleştirilecek sızma testine ilişkin detaylar aşağıda yer almaktadır.

## Bilgi Toplama Fazı

Bilgi toplama kapsamlı bir güvenlik değerlendirmesi yapabilmek için hedef hakkında olası tüm bilgileri toplamak için kullanılan evredir. İnternet üzerinden teknik (whois/dns sorguları) ve teknik olmayan (arama motorları, haber grupları, e-posta listeleri sosyal ağlar vb.) yöntemler kullanılarak, hedef şirket veya sistem hakkında bilgi sağlanabilir. Bu safhanın amacı mümkün olan her saldırı yolunu keşfederek hedef ve uygulamalarının kapsamlı bir görünümünü elde etmektir. Bu sayede hedef üzerinde bilgi güvenliğiyle ilgili her vektörün test edilebilmesine olanak sağlanır. Bu adım metodolojinin genellikle göz ardı edilen ilk ve en önemli adımlarından biridir. Diğer tüm aşamalarda olabildiğince kapsamlı ilerlenmesini sağlar.

## Network Haritalama

Birinci bölümün ardından hedefle ilgili tüm olası bilgiler edinildiğinde, hedef network ve kaynaklarını analiz etmek için daha teknik bir yaklaşım uygulanır. Network haritalama aktif bir bilgi toplama aşamasıdır. Bu evrede amaç; hedef sistemin muhtemel bir network topolojisinin üretmek ve network yapısının detaylandırılmasıdır. Bu aşamada; hedef sistem üzerinde port ve servis taraması, açık sistemlerin belirlenmesi, açık sistemler üzerindeki açık portların ve servislerin belirlenmesi, sistemler üzerinde hangi işletim sistemlerinin ve servislerin çalıştığının belirlenmesi, işletim sistemlerine, servislere ve uygulamalara ait versiyon bilgilerinin tespiti, sistemlerde kullanılan donanım/yazılımların ve versiyonlarının tespit edilmesi, Router, Firewall, IPS gibi ağ cihazlarının tespiti gerçekleştirilerek detaylı bir network haritası çıkarılır. Network haritalama bilgi toplama aşamasından elde edilen bilgilerin doğrulanmasına yardımcı olarak, hedef sistemler ile ilgili bazı bilgi elde edilmesini sağlayacaktır.

## Enumerating Fazı

Bu aşamada bir önceki adımda canlı olduğu tespit edilen sistemler üzerinde TCP/UDP port tarama işlemi gerçekleştirilir. Açık olduğu tespit edilen portları hangi servislerin kullandığı, bu servislerin hangi üreticiye ait servisler olduğu, versiyonları gibi bilgiler “banner grabbing” olarak adlandırılan yöntem ile öğrenilir ve manuel testler ile bu bilgilerin doğruluğundan emin olunduktan sonra bu bilgiler ışığında zafiyet veritabanları taranır ve bilinen zafiyetler sonraki aşamalarda kullanılmak üzere not alınır.

Tespit edilen canlı sistemler içinde router, switch gibi aktif ağ cihazlarının yer alması durumunda bu cihazlar üzerinde çalışan işletim sistemleri, bu işletim sistemlerinin versiyonları, bu cihazlar üzerindeki servisler, yönlendirme protokolleri, yönetimsel amaçlı servisler ve versiyonları tespit edilmeye çalışılır ve bu bilgiler ışığında zafiyet veritabanında inceleme yapılarak sonraki aşamalarda kullanılmak üzere not alınır. Ayrıca bu cihazlar üzerinde koşan gereksiz servislerin, ön-tanımlı kullanıcı adı veya şifre bilgilerinin ya da yönetim için kullanılan güvensiz protokollerin tespiti halinde bu zafiyetler yapılandırma problemleri başlığı altında rapora yansıtılır.

## Zafiyet Tespiti Fazı

Hedef sisteme ait bilgi toplama ve network haritasının çıkarılmasının ardından, elde edilen bilgiler değerlendirilerek zafiyet analizi gerçekleştirilir. Bu aşamanın amacı, daha önce elde edilen bilgileri kullanarak zafiyetlerin varlığını teknik olarak değerlendirmektir. Zafiyet tanımlaması; network, sunucular, uygulamalar ve diğer bileşenlerdeki zafiyetleri bulmak için elde edilen verileri, çıkarılan network topolojisini değerlendirerek gerçekleştirilen güvenlik denetimini bir adım ileriye taşır. Bu aşamada hedef sisteme zarar vermeyecek şekilde zafiyetleri tanımlamak ve tanımlanan zafiyetleri bilinen istismarlarla sömürmek için çeşitli otomatize zafiyet tarama araçlarıyla taramalar gerçekleştirilebilir. Zafiyet tarama araçlarının ayarları ön tanımlı olarak kullanılmamakta ve hedef sisteme göre konfigüre edilmektedir. Tarama sonuçları Sızma Testi Uzmanı tarafından değerlendirilerek false positive ve false negatif sonuçlar elenmektedir. Zafiyet tanımlaması ve analizi sonucunda hedef sisteme sızma yolları ve senaryoları belirlenmektedir.

## Exploitation Fazı

Zafiyet analizi sonrası tanımlanan zafiyetler istismar edilmeye çalışılarak, hedef sistem ve güvenliği üzerinde denemeler gerçekleştirilir. Hedef sistem üzerindeki güvenlik önlemlerini aşılarak erişim elde edilmeye ve erişim mümkün olduğunca bağlantı (reverse, bind) sağlanmaya çalışılır. Tanımlanan zafiyetlerin istismarı için uygun PoC kodları/araçları kullanılarak veya yazılarak hedef sistem üzerinden testler gerçekleştirilir. İstismar için kullanılacak olan exploit halka açık kaynaklardan elde edilmişse hedef sistem üzerinde kullanılmadan önce klonlanmış ortamında test edilmekte ve hedef sisteme zarar verilecek işlemlerden kaçınılmaktadır.

##

## Hak Yükseltme Fazı

Erişim kazanmak bir sızma testinin odak noktasını oluşturur. Tanımlanan zafiyetler istismar edilerek hedef sistem üzerinde erişim elde edilmeye çalışılır. Erişim elde etmek için hedef sistem üzerinde tespit edilen servislerde kullanıcı adı/parola kombinasyonlarının keşfi, sistem hesaplarına yönelik boş veya varsayılan parolaların bulunması, kullanılan uygulama ve donanım cihazlarının varsayılan ayarlarda bulunması gibi zafiyetler istismar edilebilir. Hedef sisteme düşük yetkilerle dahi olsa erişim sağlandıktan sonra hak ve yetki yükseltilmeye çalışılır.

Hak ve yetki yükseltmek için erişilen hesap üzerinden çeşitli exploitler denenerek root, administrator, SYSTEM gibi yetkili kullanıcı profiline geçilmeye çalışılır.

## Web Uygulama Güvenlik Testleri

Kapsam dahilinde kurumun internet ve intranet ortamında yayın yapan web sunucuları ve web uygulamaları test edilmiştir. Web uygulamalarının aşağıdaki zafiyet türlerine göre dayanıklılığı tespit edilmeye çalışılmıştır. Kapsam dahilinde, internet bankacılığı, banka kurumsal sayfası gibi dışarı yayın yapan sunucu ve uygulamalar öncelikle test edilerek zafiyetler tespit edilmeye çalışılmıştır.

* Bilgi Toplama (Information Gathering)
	+ Spider, Robots, Crawlers
	+ Search Engine Discovery/Reconnaissance (Arama Moturu Keşfi ve Arama Motorunun Kötüye Kullanımı)
	+ Identify Application Entry Points (Uygulama Girdi Noktalarının Tespiti)
	+ Web Application Fingerprint (Uygulama İzlerinin Tespiti)
	+ Application Discovery (Uygulamanın Keşfi ve Haritalama)
	+ Analysis of Error Codes (Hata Kodlarının Analizi)
* Yapılandırma Yönetimi Testleri (Configuration Management Testing)
	+ SSL/TLS Testing
	+ DB Listener Testing
	+ Infrastructure Configuration Management Testing (Altyapı Yapılandırma Yönetimi Testi)
	+ Application Configuration Management Testing (Uygulama Yapılandırma Yönetimi Testi)
	+ Testing for File Extensions Handling (Dosya Uzantılarını İşleme Testi) Old, Backup and Unreferenced Files (Eski, Yedeklenen ve Referanslanmayan Dosya Testleri)
	+ Infrastructure and Application Admin Interfaces (Altyapı ve Uygulama Yönetim Paneli Testi)
	+ Testing for HTTP Methods and XST (HTTP ve XST Metod Testleri)
* Yetkilendirme Testleri
	+ Credentials Transport Over an Encrypted Channel (Kimlik Bilgilerinin Şifreli Kanallar Üzerinden Taşınması Testleri)
	+ Testing for User Enumeration (Kullanıcı Hesaplarının Tespitine Yönelik Testler)
	+ Testing for Guessable (Dictionary) User Account (Kullanıcı Hesaplarına Yönelik Sözlük Saldırıları)
	+ Brute Force Testing (Kaba Kuvvet Testi)
	+ Testing for Bypassing Authentication Schema (Kimlik Doğrulama Şemasını Atlatma Testleri)
	+ Testing for Vulnerable Remember Password and PWD Reset (Savunmasız Parola Hatırlatma ve Parola Sıfırlama Testi)
	+ Testing for CAPTCHA
	+ Testing Multiple Factors Authentication (Çok Faktörlü Kimlik Doğrulama Testi)
* Oturum Yönetimi Testleri
	+ Testing for Session Management Schema (Oturum Yönetimi Şeması Testi)
	+ Testing for Cookies Attributes (Çerez Niteliklerinin Testi)
	+ Testing for Session Fixation (Sabit Oturum Testi)
	+ Testing for CSRF (CSRF – Siteler Arası İstek Sahteciliği Testi)
* Kimlik Doğrulama Testleri
	+ Testing for Path Traversal (Dizin Gezinme Testi)
	+ Testing for Bypassing Authorization Schema (Yetki Şemasını Atlatma Testi)
	+ Testing for Privilege Escalation (Hak ve Yetki Yükseltme Testi)
* Veri Değerlendirme Testleri
	+ XSS (Cross Site Scripting-Çapraz Site Betik Yönlendirme) Testleri
		- Reflected XSS
		- Stored XSS
		- DOM Based XSS
	+ SQL Injection
	+ Blind SQL Injection
	+ Path Injection
	+ LDAP Injection
	+ Code Execution
		- OS Code Execution

## İstemci Tarafı Sızma Testleri

Gerçekleştirilecek denetimlerde opsiyonel olarak sunulan “İstemci Tarafı Sızma Testleri” kapsamında istemcilerin aşağıdaki zafiyet ve tehdit türlerine karşı ne kadar korunaklı olduğu tespit edilmeye çalışılır. Bu tehditlerin her biri için birer senaryo, testler öncesinde tanımlanır ve o senaryo adımları izlenerek (örneğin bir phishing mail oluşturulup kullanıcılara gönderilerek) kullanıcıların bilgi güvenli konusundaki farkındalığı ölçülmeye çalışılır.

* Spear Phishing Saldırıları
* Browser Exploit’leri
* Fiziksel Güvenlik Tehditleri

##

## Servis Dışı Bırakma Testleri

Bu kapsamda gerçekleştirilecek testler ile penetrasyon testi kapsamındaki sunucuların ve servislerin olası servis dışı bırakma saldırılarına karşı ne kadar korunaklı oldukları tespit edilmeye çalışılır. Kontrollü bir şekilde gerçekleştirilecek bu servis bırakma saldırıları hem uygulama katmanında hem de network katmanında yapılır.

Bu aşamada isteğe bağlı olarak aşağıdaki DoS türlerinin testleri gerçekleştirilir.

* SYN Flood
* HTTP GET/POST Flood

## Veritabanı Zafiyet Testleri

Opsiyonel olarak sunulan bu test adımında veritabanlarına özel güvenlik taramaları gerçekleştirilir. Bu adım, veritabanına bir kullanıcı ile bağlanmayı gerektirdiğinden dolayı çalışma öncesinde bir veritabanı kullanıcısının oluşturulmuş olması ve ilgili veritabanları üzerinde gerekli hakların bu kullanıcıya tanınmış olması gerekmektedir.

Yapılan zafiyet taramaları sırasında veritabanları üzerindeki varsayılan konfigürasyondan kaynaklı zafiyetlerden eksik güncüllemelere, gereksiz yetki tanımlarından ön tanımlı şifrelerin tespitine kadar birçok veritabanı sistemlerine özel açıklıklar tespit edilebilmektedir.

## Kablosuz Ağ Sızma Testleri

Opsiyonel olarak sunulan bu test adımında kapsamındaki wireless sistemleri için asgari aşağıdaki güvenlik denetimleri gerçekleştirilir.

* WLAN Tanımlama ve Kapsama Haritası Çıkarma
* WLAN Şifre Tespiti ve Şifre Kırma
* WLAN Dinleme ve Araya Girme
* WLAN Zayıflık Tarama

##

## Raporlama

Gerçekleştirilen güvenlik denetiminden sonra takip eden 10 (on) iş günü içerisinde biri yönetici diğeri teknik olmak üzere hazırlanan iki rapor şifreli halde kuruma e-posta ile teslim edilir. Kurum tarafından istenmesi durumunda raporun matbu hali, üzerine “**Gizli**” ibaresi vurulmuş kapalı bir zarf içinde teslim edilir.

Teslim edilecek rapor aşağıdakileri içerir;

* Gerçekleştirilen güvenlik denetim çalışmasına ve bulgulara ilişkin yönetici özeti
* Test sırasında tespit edilen zafiyetlerin kritiklik seviyelerini, hangi sistemlerde bu zafiyete rastlandığını gösteren ve zafiyeti ortadan kaldırmaya yönelik çözüm önerilerinin bulunduğu zafiyet kimlik kartları

Teslim edilecek raporların yanında zafiyetlerin giderilip giderilmediğinin takibini kolaylaştırmak adına tespit edilen zafiyetlerin ve bu zafiyetlerin bulunduğu sistemlerin bilgisinin yer aldığı bir Excel dokümanı kuruma verilir ve doğrulama denetiminde bu dokümandaki bilgiler baz alınır.

##

## Sunum

Raporların tesliminden sonra istenmesi halinde kurum personeline, gerçekleştirilen sızma testine ilişkin özet mahiyetinde bir sunum yapılır. Bu sayede kurum personeli, sızma testini gerçekleştiren uzmanlarımızla test ile ilgili görüş alışverişinde bulunabilme imkânı kazanırlar.