SİBERAY SÖZLÜK

A

- Adli Bilişim (Computer Forensics) : Bilişim cihazları üzerinde araştırma, inceleme, tespit vs. işlemler yapan hukuk alı, alanı ve faaliyetidir. Bu tür işlemler ile gerek kolluk kuvvetlerinin gerekse yargı makamlarının bilişim alanındaki delil ihtiyacı sağlanmaktadır.

- Adli İnceleme (Digital Forensics) : Bir cihazın, çeşitli teknikler kullanılarak ve gerektiğinde yardımcı cihazlar ile araç-gereçlerden yararlanılarak adli amaçlarla incelenmesi işidir. Bu işlemin amacı bir siber güvenlik olayının meydana geldiğini veya kimler tarafından gerçekleştirildiğini belirleyebilmektir.

- Ağ (Network) : İki veya daha fazla bilgisayarın, kablolu ya da kablosuz iletişim araçları ve yazılım-donanım bileşenleri arasında bağlantı kurulmasıyla oluşturduğu sisteme verilen isimdir.

- Ağ dinleme (Sniffing) : Ağ dinleme araçları kullanarak ağdan geçen tüm veri paketlerini yakalayıp izlenmesi sürecidir. Sniffing işleminin yapılabilmesi için uzman seviyesinde bilgisayar, güvenlik ve ağ bilgisine ihtiyaç bulunmaktadır.

- Alan Adı Sistemi (Domain Name System / DNS) : Bilgisayarlar arasında iletişimi sağlamak amacıyla oluşturulmuş protokollerdir. Bu kapsamda bir kullanıcının kendi bilgisayarı ile başka bilgisayarlarla iletişime geçebilmesi için, iletişim kurulmak istenen bilgisayarın internet protokol adreslerini bilmesi gerekecektir. İletişime geçilecek tüm bilgisayarların IP numaralarını akılda tutmak zor olduğu için alan adı sistemi olarak adlandırılan DNS protokolü geliştirilmiştir.

- Anonim Proxy (Anonim Vekil) : Kullanıcının internet üzerinden gerçekleştirdiği hareketliliği gizlemesini sağlayan yazılımdır.

- Anti-malware : Bilgisayar virüsleri, solucanlar, trojanlar, zararlı tarayıcı eklentileri, adware ve Spyware dahil olmak üzere birçok malware tehdidini tespit etmek veya ortadan kaldırmak için yaygın olarak kullanılan teknolojidir.

- Asılsız metinler / Uyarılar (Hoax) : Asılsız Metinler, toplumu korkutmak, dolandırmak veya eğlendirmek amacıyla yazılan ve internet üzerinden yayımlanan hikayelerdir. Hoax'lar bireyleri yanlış yönlendirmek ve dolandırmak amacıyla, asılsız ve yanlış havberler içeren metinler şeklinde hazırlanırlar. Hoax'lar para talebinde bulunmak veya kullanıcı bilgisayara zararlı yazılım yüklemek amacıyla kullanılabilirler. Örneğin; "bu mesajı yüz kişiye dağıtmanız halinde, bu durum size şans getirecektir" şeklinde bir e-posta asılsız metin olarak tanımlanabilir.

- Avrupa Konseyi Sanal Suçlar Sözleşmesi (Council of Europe Conwention on Cybercrime) : Avrupa Konseyi Sanal Suçlar Sözleşmesi veya Sanal Ortamda İşlenen Suçlar Sözleşmesi, bilgisayar suçlarını ve internet suçlarını gözeten ilk uluslararası sözleşmedir.
  Türkiye 10 Kasım 2010 tarihinde Avrupa Konseyi Sanal Suçlar Sözleşmesi'ni Strasbourg'da imzalamıştır.

B

- Barındırma Alanı (Web Server Hosting) : Barındırma Alanı, web sitesi sahibi olmak isteyen internet kullanıcılarına internetten alan sahibi olma imkanı sağlayan sistematiktir. Her web sitesinin boyutuna göre kapladığı bir alan vardır ve internette barınabilmek için bu alanı hosting hizmeti ile karşılamaları gerekir. Bu hizmet, şirketlerin sunucuları sayesinde gerçekleşir. Kullanıcılar, sunucuların tamamını veya bir kısmını ihtiyaçlarına göre kiralayabilir. Devreye aracı şirketler veya ortak sunucu paylaşımı gibi etkenler girince güvenlik sorunları da kaçınılmaz olur. Bununla birlikte, bir barındırma alanı seçilirken özellikle sunucuların güvenliğine dikkat edilmelidir.

- Bilgi Güvenliği (Information Security) : Bilgilerin korunması amacıyla oluşturulan faaliyetlerin bütünüdür. Bu kapsamdaki faaliyetler ile bilgilerin manipüle edilmesi, ifşa edilmesi, ele geçirilmesi ve/veya zarar görmesi engellenir.

- Bilgi Güvenliği Yönetim Sistemi (Information Security) : Bilgilerin korunması amacıyla oluşturulan faaliyetler bütünüdür. Bu faaliyetlerin sistemli, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, kurumun/kuruluşun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı bir usul ve tarzda planlanması gerekir.

- Bilgi Teknolojileri ve İletişim Kurumu / BTK : Türkiye'de sekteröl bakımdan, telekomünikasyon sektörünü düzenleyip denetleyen ilk kurumdur.

- Bilgisayar Korsanı (Hacker) : Yazılım konusunda teknik becerileri olan kişileri tanımlamak için kullanılabilir. Ancak genellikle suç işlemek amacıyla sistemlere veya ağlara yetkisiz erişim sağlamak için yeteneklerini kullanan bir kişi anlamına gelir.
    - Siyah Şapkalı Hacker : Kişi veya kurumlara ait bilgisayarların, telefonların veya ağların güvenlik sistemlerine izinsiz olarak sızan ve bunu kendi menfaatleri doğrultusunda kullanan kişiler
    - Beyaz Şapkalı Hacker : İyi niyetli olarak faaliyet gösteren bilgisayar korsanlarıdır. Etik Bilgisayar Korsanları
    - Gri Şapkalı Hacker : Sahibinin izni veya bilgisi olmadan, bir sistemdeki güvenlik açıklarını arayan hackerlardır. Sorunları bulmaları halinde, bunları sahibine bildirir ve bazen sorunu çözmek için ücret talep edebilirler.

- Bilişim Sistemleri (Information System) : Ağ teknolojileri vasıtasıyla sağlanan tüm hizmet ve faaliyetlerin sunumunda kullanılan sistemleri tanımlayan kavramdır.

- Bulut (Cloud) : Bilgilere erişimi sağlayan ve bunları depolayabilen internet tabanlı veri depolama sistemidir.

- Bütünlük (Integrity) : Bilgisayar sistemlerinde bilgilerin kasıtlı olarak, yetkisiz bir erişim sağlanmasıyla veya bir kaza/hata sonucu değişikliğe uğraması söz konusu olabilmektedir. Bu tür handikapların ve sorunların ortaya çıkmasını engellemek amacıyla da çeşitli koruma sistemleri kullanılabilir. Bu koruma sistemleri ise Bütünlük olarak tanımlanmaktadır.

- Büyük Zombi PC Ağı (Botnet) : Hackerlar tarafından ele geçirilmiş internete bağlı bir bilgisayar ağına zombi bilgisayar denir. Genellikle zombi bilgisayarlar, bir botnet'e bağlıdır ve internet üzerinde zararlı eylemleri gerçekleştirmek üzere kullanılırlar. Botnet aynı komutları gerçekleştiren zombi bilgisayarların oluşturduğu bir ağ şeklinde tanımlanabilir.

C

- Casus Programlar (Spyware) : Bilgisayarlara yönelik olarak casusluk yapmak amacıyla tasarlanmış yazılımlardır. Kullanıcılara ait bilgilerin veya işlemlerin, yetkisiz bir şekilde toplanmasını ve ilgisiz kişilere gönderilmesini sağlarlar.

- Cyber Grooming : Sanal ortamda çocuklar ile iletişime geçerek onları istismar etmek veya onlardan cinsel anlamda fayda sağlamak amacıyla çocuklarla yaklaşmak, çocuklara karşı kendilerini olmadıkları gibi göstermek, çocuklarla arkadaşlıklar kurmayı ifade etmektedir.

Ç

- Çerez (Cookie) : Çerezler, ziyaret edilen internet siteleri tarafından tarayıcılar aracılığıyla cihazlara veya ağ sunucularına depolanan küçük metin dosyalarıdır. İnternet sitelerinde çerez kullanılmasının amacı, internet sitesinin işlevselliğini ve performansını arttırarak, sunulan hizmetleri geliştirmek, internet üzerinden yeni özellikler sunmak ve sunulan özellikleri kullanıcıların tercihlerine göre kişiselleştirmektir. Çerez kesinlikle bir virüs değildir.

- Çevrim İçi Kandırma (Online Enticement) : Bir kişinin çocuk olduğuna inandığı kişi ile internet aracılığıyla iletişim kurup, çocuğu kaçırma veya ona karşı cinsel istismar suçu işlemesidir.

- Çocuk Koruma Sistemi (Child Protection System) : P2P yöntemi ile çocuk istismarı görüntülerinin paylaşılması durumunda paylaşımda bulunan istismarcıları tespit etmeye yönelik çalışmalar yapılmasını sağlayan CRC tarafından üretilen bir programdır.

- Çok Faktörlü Kimlik Doğrulaması (Multi - Factor Authentication) : Bir kimlik belgesini kanıtlamak için birden çok kimlik doğrulama faktörü kullanılmasıdır. Bir kimlik doğrulama girişiminde sunulan bileşenlerin en az biri eksik veya yanlış ise kullanıcının kimliği yeterli derecede kesin değilse veya varlığa erişim sağlanmazsa erişim engellenebilmektedir. Güvenlik sistemlerine entegre edilerek mevcut güvenlik sistemlerinin bir adım daha güvenli kılınmasına imkân sağlamaktadır.

D

- Dağınık Hizmet Engelleme: Distributed Denial of Service (DDoS) olarak bilinen bu siber saldırı yönteminde, ilk aşamada kötü amaçlı yazılımlara çok sayıda bilgisayar aynı anda ele geçirilmekte ve bu bilgisayarlar “zombi” bilgisayar haline getirilmektedir. Bu aşamada çoğu zaman kullanıcılar, bilgisayarlarının ele geçirildiğinin farkında olmamaktadırlar.

İkinci aşama da ise ele geçirilen bu bilgisayarlardan "Botnet" adı verilen bir ağ oluşturarak, önceden planlı bir şekilde hedeflenen web sayfalarına sistematik olarak saldırmak suretiyle, hedef alınan ağ sistemlerini kullanılmaz hale getirmektedir.

- DNS Korsanlığı: İnternet kullanıcılarının erişmeye çalıştıkları adres yerine başka bir internet adresine yönlendirmesine yönelik süreçlerin bütününü ifade eden bir kavramdır. Bu süreçler çeşitli kötü amaçlı yazılımlar kullanılarak, bir sunucunun TCP/IP ayarları değiştirilmesi ile söz konusu olur. Böylelikle kullanıcılar siber saldırgan tarafından tasarlanmış sahte bir DNS sunucusuna ulaştırılır. Bu kapsamda da siber saldırgan özellikle e-dolandırıcılık gibi bir hedefle kullanıcıların mağdur edilmesine neden olur.

E

- Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı (The General Directorate of Security Department of Combating Cyber Crimes): Bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli Daire Başkanlıkları ile birimlerin dağınık yapısının tek bir çatı altında toplanması, mükerrer yatırımların önüne geçilmesi, siber suçlarla etkin ve verimli bir şekilde mücadele edilebilmesi amacıyla 2011/2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. Daha sonra ise 28/02/2013 tarihli Bakanlık Oluruna istinaden Bilişim Suçlarıyla Mücadele Daire Başkanlığı'nın ismi Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir.

- Eradikasyon (Eradication) : Bir siber olayın ortadan kaldırılma sürecidir. Bu süreç, siber olayın tespiti, kontrolü ve tüm sonuçları ile bertaraf edilmesi şeklindedir.

- Erişilebilirlik (Accessibility) : Bilgilere, yetkili kişilerin ihtiyaç halinde ulaşabilmesinin temin edilmesidir.

- Erişim Kontrolü (Access Control) : Bir yeri veya kaynakları kimlerin veya nelerin görüntüleyeceğini, kullanabileceğini veya erişebileceğini düzenleyen bir güvenlik tekniğidir Riski en aza indirmek için tasarlanmış bir bilgi güvenliği uygulamasıdır.

F

- Fidye Yazılımı (Ransomware) : Şantaj yazılımı veya fidye virüsü olarak bahsedilen yazılımlara verilen kötü amaçlı yazılımların genel adıdır. Bunların amacı mağdur kullanıcının bilgisayarındaki dosyaları şifreleyerek, ilgilinin dosyalarına tekrar erişebilmesi için karşılığında bir fidye-ücret ödemeye zorlanmasıdır.

G

- Gelişmiş Şifreleme Standardı (Advanced Encryption Standard) : 128 ila 256 bit anahtar boyutlarını kullanan simetrik bir şifreleme algoritmasıdır.

- Gizlilik (Privacy) : Bilişim sistem ve verilerine, sadece yetkili kişi veya sistemlerce erişilebilmesi şeklinde tanımlanabilir. Bir başka tanımda ise bilinmesi gerekenler bazındaki bilgilerin, sadece yetkili kişilerin süreçlerin veya sistemlerin erişimine açık olmasını öngören en düşük erişim hakkı prensibi olarak da ifade edilmektedir.

- Güç Dağılımı (Diffusion of Power) : Joseph Nye tarafından ortaya atılan bir kavramdır. Söz konusu kavram ile süreç içinde siber uzaya devletlerin tek başlarına hakım olamayacakları, siber uzaydaki gelişmeler kapsamında gücün büyük devletlerden görece daha küçük devletlere ve devlet dışı aktörlere (hacker grupları, bireyler, örgütler vb.) kayacağı ileri sürülmektedir.

- Güvenli Kabuk (Secure Shell) : Ağ hizmetlerinin güvenli olmayan bir ağ üzerinde, güvenli şekilde çalıştırılması için kullanılan bir kriptografik ağ protokolüdür.

- Güvenli Soket Katmanı (Secure Sockets Layer) : Bilgisayar ağı üzerinden güvenli haberleşmeyi sağlamak için tasarlanmış kripto protokolleridir.

- Güvenlik Açığı (Security Bug) : Sistem üzerindeki yazılım ve donanım hatalarından kaynaklanan zafiyet noktalarıdır.

- Güvenlik Duvarı (Firewall) : Siber saldırganları, yazılım ve donanımlardan uzak tutmak için tasarlanmış siber güvenlik teknolojileridir. Güvenlik duvarları donanım veya yazılım tabanlı olarak tasarlanabilir.

H

- Hacklemek (Hacking) : Kullanılan donanım sistemi hakkında genel bilgi toplamak, sahip olduğu tüm verilere ulaşmak ve kopyalamak amacıyla, sistem açıklarından faydalanarak, ilgili donanıma internet yoluyla izinsiz giriş yapılması olayına hacking adı verilir. Hacking olayını gerçekleştiren kişi de hacker olarak tanımlanmaktadır.

I/İ

- IP Güvenliği (IP Security) : Bir veri akışındaki her IP paketinin şifrelenmesi ve tanımlanması yoluyla, tüm iletişimin güvenliğini sağlamak için oluşturulmuş protokoller takımıdır.

- IP Hırsızlığı (IP Spoofing) : Bir sisteme veya ağa izinsiz erişim sağlamak için sahte IP adresi kullanılmasıdır.

- İçerik Filtreleme (Content Filtering) : İnternet üzerindeki içeriklerinin analiz edilerek, ağa erişimin kontrol edilmesi ve gerektiğinde engellenmesidir.

- İki Faktörlü Doğrulama (Two-Factor Authentication) : Doğrulama için iki bağımsız mekanizmanın kullanılmasıdır.
- İnternet Değişim Noktası (Internet Exchange Point) : İki bağımsız otonom sistemin birbirine bağlanması suretiyle internet trafiğinin değişimine imkan veren altyapıdır.

- İyileştirme (Remediation) : Zafiyet teknolojileri temelli kritik iş süreçlerinin akamete uğraması halinde kurum tarafından uygulanan plandır.

- İzinsiz Giriş Önleme Sistemi (Intrusion Prevention System) : Bir kuruluşun internet altyapısı üzerinden gerçekleşen trafiğin siber saldırılara karşı korunması gerekmektedir. Bu kapsamda söz konusu koruma fonksiyonunu yerine getiren sistemlere verilen isimdir. Bu sistem ilgili kuruluşun internet trafiğini sürekli olarak kontrol eder, bir ihlal görmesi halinde bunu engeller ve sorumlu birime haber verir.

- İzinsiz Giriş Tespit Sistemi (Intrusion Detection System) : Ağ üzerindeki trafiği sürekli olarak izleyen, şüpheli bir durumla karşılaştığında ağ yöneticisine uyarı gönderen ve güvenlik duvarı üzerindeki ilgili tarfiği kapatarak güenliğini sağlayan sistemdir.

- İzleme Politikası (Monitoring Policy) : Bir kuruluşun bilgisayarları, ağları ve uygulamalrına ilişkin süreçlerin takip edilmesi ve bu kapsamda ilgili kurumun siber güvenliğinin sağlanması için gerekli amaç ve planlardır.

K

- Kaba Kuvvet Saldırısı (Brute Force Attack) : Deneme yanılma yönetimi kullanarak bir parola veya kullanıcı adını ele geçirme, gizli bir web sayfasını bulma ya da bir mesajı şifreleme amacıyla kullanılan anahtarı arama girişimidir.

- Kimlik Doğrulama (Authentication) : İnternet temelli bir sistemin kullanıcılarının kimliğini ve bilgilere erişim yetkisinin doğrulanmasıdır.

- Kişisel Bilgilerin Korunması (Personal Information Protection) : İnternet ve sosyal medya uygulamaları ile ilgili süreçler kapsamında, kişisel bilgilerin korunması amacıyla alınan tedbirlerin tümünü ifade eden bir kavramdır.

- Kriptanaliz (Cryptanalysis) : Kriptanaliz işlemi kriptografi kullanılarak şifre edilmiş bir verinin şifresini çözme, yani veriyi analiz etme işlemidir.

- Kriptografi (Cryptography) : Bilginin istenmeyen şahıslar tarafından anlaşılmasını önlemek ve gizliliğini sağlamak amacıyla şifrelenmesinde kullanılan teknikler bütünüdür.

- Kriptoloji (Cryptology) : Şifre bilimidir. Belge ya da mesajın şifrelenip istenilen yere iletilmesi ve ardından deşifre edilmesini sağlama faaliyetiyle uğraşan bilim dalıdır.

- Kurtarma (Recovery) : Siber olay sonrasında oluşan hasarı, geri döndürmek amacıyla yapılan müdahale sürecidir.

M

- Mantıksal Erişim Kontrolleri (Logical Access Controls) : Bir sistem üzerinde kullanıcı erişimleri kullanılmak suretiyle uygulanan kontrol süreçleridir. Bu süreçler, söz konusu erişimlerin uygulanması, izlenmesi, düzenlenmesi, test edilmesi ve sonlandırılması aşamaları üzerinden icra edilir.

- Maskeleme (Masking) : Şifreler gibi hassas bilgilerin görünürlüğünü gizleyen uygulamalardır.

- Metasploit : Güvenlik açıkları hakkında bilgi sağlayan, sızma testleri ve IDS imza gelişmesinde yardımcı olan bir bilgisayar güvenlik projesidir.

N

- Nesnelerin İnterneti (Internet of Things / IoT) : Benzersiz bir şekilde adreslenebilir nesnelerin kendi aralarında oluşturduğu, dünya çapında yaygın bir ağ ve bu ağdaki nesnelerin belirli bir protokol ile birbirleriyle iletişim içinde olmaları
  Nesneler, algılayıcılar ve elektronik devreler ile donatıldığında insanlarla iletişime geçerek, durum bilgilerini güncelleyebilecek yetenekler kazanırlar. Mobil ağlar ve internetin gelişimiyle birlikte bu nesnelerin kişiler ile iletişim kurmaları kolaylaşmıştır ve insanlar da onları her yerden, her zaman gözlemleme ve kontrol etme şansına sahip olmuştur.

O

- Olay Müdahalesi (Incident Response) : Bir işletmede bir siber güvenlik olayı meydana geldiğinde, ortaya çıkan hasarın giderilmesi için önceden hazırlanan iş süreçleridir.
- Oltalama (Phishing) : Teknolojik imkanlardan faydalanılarak oluşturulan özel yöntem ve içeriklerle, insanların kişisel/hassas bilgilerini ele geçirmeyi amaçlayan bir dolandırıcılık türüdür.
- Omuz Sörfü (Shoulder Surfing) : Parola yazılırken ya da erişim kısıtlı sistemlere erişilirken kurbanın izlenmesidir. Omuz sörfüne maruz kalabilecek olası yerler; havaalanları, kafeler, oteller ve kamuya açık alanlar gibi müşterek kullanılan internet ağlarıdır.

- Orta adam saldırısı (Man-in-the-Middle Attack / MİTM) : Aradaki adam saldırısı olarak da tanımlanabilmektedir. En genel ifadeyle, siber saldırganların, bir ağ üzerinde hedef bilgisayar ile diğer ağ araçları arasında çeşitli siber saldırı yöntemleri ile girerek, gerçekleşen iletişime dair verileri yakalama ve şifrelenmemiş verileri görebilme ilkesine dayanan bir saldırı çeşidi olarak tanımlanabilir.

P

- Paket Filtreleme (Packet Filtering) : Hangi çeşit ve türdeki internet trafiğinin gönderileceğinin veya alınacağının belirlenmesi süreçleridir.

- Protokol : İki ya da daha fazla bilgisayar arasındaki iletişimi sağlamak amacıyla verileri düzenlemeye yarayan kurallar bütünüdür.

R

- Risk Değerlendirmesi (Risk Assessment) : Siber risklerin ve olası risk kaynaklarının etkilerini değerlendirme sürecidir.

- Risk Kabulü (Acceptance Risk) : Bir kurumun tolerans gösterebileceği siber risk seviyesidir.

- Risk Toleransı (Risk Tolerance) : Yönetimin kabul edebileceği siber risk seviyesidir.

- Risk Transferi (Risk Transfer) : Siber riskin gerçekleşmesi ile birlikte ortaya çıkan somut hasarların bir başka aktöre aktarılmasıdır.

- Riski Önleme (Risk Avoidance) : Siber riski engelleyerek, olası hasarlardan kaçınma sürecidir.

- Riskin Azaltılması (Risk Mitigation) : Siber riskin yönetilmesi amacıyla alınan etkili tedbirlerdir.

S

- Sahte Antivirüs Yazılımı (Fake Antivirus) : Siber saldırılara karşı güvenlik açısından yararlı gibi görünen, fakat etkisiz güvenlik sağlayan yazılımlardır.

- Saldırı Önleme Sistemi (Intrusion Prevention System) : Bir kurumun siber güvenlik açığı ihlallerini tespit etmek amacıyla internet trafiği süreçlerini izleyen sistemlerdir.

- Sanal Ağ Geçidi (Virtual Gateway) : Kurum içi veya VNet-VNet bağlantısı için eşlenen sanal ağda VPN ağ geçidinin kullanılmasına imkan sağlayan bir eşleme özelliğidir.

- Sanal Özel Ağ (Virtual Private Network / VPN) : İnternette gerçekleştirilen her harekette dijital izler bırakmadan, mahremiyeti koruyarak, kısıtlı olmaksızın tüm internet sitelerine özgürce erişim sağlamayı temin eden bir alt yapıdır.

- Savunmasız Bölge (Demilitarized Zone / DNZ): Siber güvenlik tedbirleri vasıtasıyla tam anlamıyla korunmayan/korunamayan alanlardır.

- Sınır Güvenliği (Border Security) : Bilişim sistemlerinin, güvenlik duvarı ve saldırı engelleme sistemleri gibi erişim kontrolü sağlayan sistemler aracılığı ile dış ağlardan gelebilecek saldırılardan korunması.

- Sızma Testi (Penetrasyon Test) : Kurumların bilişim altyapısına yönelik saldırılara karşı güvenlik açıklarını tespit edebilmek amacıyla yapılan güvenlik testleridir.

- Siber Aktivistler (Cyber Activists) : İnternet üzerinden gerçekleştirilen eylemlere katılarak siyasi ve toplumsal bir olaya destek vermek amacıyla faaliyet gösteren kimseleri ifade etmektedir. Siber aktivistler, örneğin bir online dilekçe imzalama veya bir sosyal medya web sitesinde bir kampanya grubuna katılma, retweet etme, hashtag oluşturma gibi etkinlikler planlarlar.

- Siber Çatışma (Cyber Conflict) : Önemli bir hasar veya yıkım yaratmak için bir başka ülkenin bilgisayar sistemlerini bozmak amacıyla dijital saldırı kullanılması durumunu ifade eden kavramdır.

- Siber Devriye (Cyber Patrol) : Siber Devriye, Emniyet Genel Müdürlüğü bünyesinde 2011'de kurulan Siber Suçlarla Mücadele Daire Başkanlığı ile bu başkanlığa bağlı yerel birimlerin, internetin suçlulardan arındırılması için 7 gün 24 saat esasıyla sanal ortamda yaptıkları devriye faaliyetidir.

- Siber Güvenlik (Cyber security) : Siber kaynaklı saldırılara, tehditlere, sabotajlara ve terör faaliyetlerine karşı kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan politikalar, oluşturulan güvenlik kavramları, risk yönetimi yaklaşımları gibi faaliyetlerin tamamıdır.

- Siber Olay (Cyber Event) : Siber uzay kaynaklı saldırılar, tehditler ve sabotajların her birine siber olay denir.

- Siber Ortam (Cyber Area) : Kara, deniz, hava ve uzaya yayılmış durumda bulunan bilişim sistemleri ile bunları birbirine bağlayan ağların bütününe siber ortam denir.

- Siber Risk (Cyber Risk) : Siber olayın olumsuz sonuçlarına ilişkin olasılıklar kombinasyonudur.

- Siber Savaş (Cyber War) : Bir devletin kritik altyapılarına ve bilgisayar sistemlerine zarar vermek veya kesintiye uğratmak amacıyla gerçekleştirilen faaliyetler bütünüdür.

- Siber Savunma (Cyber Defense) : Bilişim sistemlerini veya kritik altyapıları, siber tehditlere karşı korumak amacı ile alınan önlemlerdir.

- Siber Suç (Cyber Crime) : Bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzay kaynaklı olarak çeşitli tehdit odaklarından gelen ve kanunlara göre suç kabul edilen eylemlerdir.

- Siber Uzay (Cyberspace) : Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam.

- Siber Varlık (Cyber Value) : Siber uzay kaynaklı potansiyel risk ve saldırılara karşı korunması gereken değerli bilgi kaynaklarının bütünüdür.

- Siber Vatan (Cyber Homeland) : Bir ülkenin kendi siber uzay alanında sahip olduğu egemenlik haklarını ifade etmektedir.

- Siberay Projesi (Siberay Project) : İçişleri Bakanlığı ve Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı bünyesinde geliştirilen ve toplumda siber güvenlik farkındalığı yaratmayı amaçlayan bir projedir. Siberay programının temel amacı güvenli internet kullanımı için kullanıcılara ve vatandaşlara yol göstermektir. Ayrıca bu proje, ulusal ve uluslararası platformlarda, siber güvenlik, teknoloji kullanımı, sosyal medya kullanımı, siber zorbalık ve teknoloji bağımlılığı gibi konularda farkındalık oluşturarak; internete, ekran, teknoloji bağımlılığı gibi kişiye ve topluma zarar veren alışkanlıklarla, siber zorbalıkla ve her türlü siber suçlarla eylem daha oluşmadan mücadele etmektedir. Programın bir diğer amacı, toplumun her bir ferdinin interneti ve teknolojiyi güvenli, faydalı, etkili şekilde kullanmalarını sağlamaya yönelik faaliyetler, içerikler, çalıştaylar, çevrimiçi ve çevrimdışı konferanslar düzenleyerek bilinçli nesiller yetiştirilmesine katkı sağlamaktır.

- Solucanlar (Worms) : kendi kaynak dosyalarını hızlı bir şekilde diğer kullanıcılara da ulaştırmayı denerler ve bu yolla kendilerini çok fazla sayıda çoğaltabilirler.

- Sosyal Mühendislik (Social Engineering) : Siber uzay kaynaklı olarak insanları yönlendirmek veya gizli bilgileri ifşa etmek suretiyle yapılan psikolojik manipülasyondur.

- Spam e-posta (Spam E-Mail) : Spam kelime anlamı olarak “istenmeyen” anlamına gelmektedir. Bu kapsamda istenmeyen e-postaları ifade eden bir kavram olarak bilinmektedir.

- Spearphishing : Hedef odaklı yemleme olarak adlandırılan bu saldırı türü belirli bir kuruluş içindeki kişilerin hedef alınarak kritik bilgileri paylaşmaları konusunda yanıltma ve tuzağa düşürmeye yönelik elektronik postaların gönderilmesini ifade etmektedir.

S

- Şifre (Password) : Gizliliği olan sistemlerin açılması, kullanılması veya iletilmesi için gerekli olan harf, rakam, sembol vb. verilerin bir bütünüdür.

- Şifre Çözme (Decryption) : Siber uzayda gizliliği temin etmek amacıyla tasarlanan şifrelerin erişilebilir hale getirilmesidir.

- Şifreleme (Encryption) : Siber uzayda gizliliği temin etmek amacıyla imgeleri, sözleri, harfleri ve rakamları tasarlama işlemidir.

T

- Tek Faktörlü Doğrulama (Single Factor Authentication / SFA) : Bir bilgisayar kullanıcısı için kullanıcının kimlik doğrulama mekanizmasının tek bir süreci içermesi durumudur.

- Tıklama Korsanlığı Saldırısı (Clickjacking Attack) : İnternet kullanıcılarının iradeleri dışında veya manipüle edilerek bir bağlantıyı tıklamalarını sağlayan saldırı çeşididir.

- Truva Atı (Trojan) : Zararlı kod içeren virüs anlamında kullanılır. Kullanıcıya faydalı bir program gibi görünen bu yazılım, çalıştırıldığında hedef sisteme çeşitli zararlar vermektedir.

- Tuş Kaydedici (Keylogger) : Bir donanıma nüfuz ettirilmesiyle birlikte aktif hale gelen tuş takip programlarıdır. Bu kapsamda kullanıcın klavyesine her basıldığında, bu uygulama her tuşu bir dosyaya kaydeder. Kelogger, eğer sistem yöneticisinin bilgisi dahilinde yüklenmişse, tamamen sistem güvenliği için çalışmaktadır. Fakat bu yazılım sistem yöneticisinin bilgisi olmadan yüklenmişse, tamamı ile saldırı ve casusluk amacı taşır.

U

- Ulusal Siber Güvenlik (National Cyber Security) : Ulusal siber ortamda bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem ve verinin, ayrıca bunların sunumunda yer alan sistemlerin siber güvenliğini ifade etmektedir.

- Ulusal Siber Olaylara Müdahale Merkezi / USOM, TR-CERT (National Cyber Events Response Center) : Türkiye'nin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerinin azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde oluşturulmuş olan yapılanmadır.

- Ulusal Siber Ortam (National Cyber Area) : Bir devletin kamu bilişim sistemleri ile gerçek ve tüzel kişilere ait bilişim sistemlerinden oluşan dijital ortamdır.

- Ulusal Siber Uzay (National Cyberspace) : Kamu bilişim sistemleri ile gerçek ve tüzel kişilerce iletilen/kullanılan bilişim sistemlerinden oluşan ortamdır.

- URL Yanıltma (URL Spoofing) : Kullanıcıların, yanıltılarak veya maniplüe edilerek bir web sitesine ait URL'yi tıklamaları ve bunun sonucunda istemedikleri farklı adreslere yönlendirilmeleridir.

- Uygulama Katmanı (Application Layer) : Ağ ve uygulama arasında arabirim işlevini yerine getiren mekanizmadır.

- Uyumluluk (Compliance) : Siber uzayda kamu ve özel hukuk kapsamındaki yükümlülüklerin kullanıcılar tarafından yerine getirilebilme yeteneğidir.

- Uzaktan Erişim Servisi (Remote Access Service / RAS) : İnternet üzerinden kullanıcıların bilgisayarlarına bağlanılmasını sağlayan servislerdir.

V/W

- Vekil Sunucu (Proxy Server) : İnternete erişim sırasında kullanılan bir ara sunucudur. Bu kapsamda internet üzerindeki bir bilgisayar ile internete bağlı diğer bilgisayarlar arasındaki iletişimi sağlayan yardımcı bir geçiş yolu sistemi olarak da tanımlanabilmektedir.

- Veri Hırsızlığı (Data Theft) : Bilgilerin kötü niyetli hackerlar tarafından çalınmasıdır.

- Veri Kaybı (Data Loss) : Verilerin hatalı işlemler sonucu kısmen veya tamamen kaybedilmesi halidir.

- Veri Madenciliği (Data Mining) : Büyük ölçekli veri yığını içerisinde işlenmeye uygun faydalı verilerin ayrıştırılmasıdır.

- Veri Saklama Politikası (Data Retention Policy) : Bir kuruluşa ait verilerin yasal bir çevre ve kurum kültürü kapsamındaki kurallar dahilinde muhafaza edilmesidir.

- Veri Sızıntısı (Data Leakage) : Verilerin tamamının veya bir kısmının hatalı veya kasıtlı uygulamalar neticesinde yanlış hedefe gönderilmesi çalınması, kaybedilmesi veya sızdırılmasıdır.

- Veri Şifreleme Standardı (Data Encryption Standard) : İkili verilerin şifrekenmesi için algoritmadır.

- Virüs (Virus) : Bilgisayarın çalışmasını engelleyecek, verileri kaydedecek, bozacak veya silecek ya da kendilerini internet üzerinden diğer bilgisayarlara yayarak yavaşlamalara veya başka sorunlara neden olacak şekilde tasarlanmış yazılımlardır.

Y

- Yama (Patch) : Yazılım programlamaları yapılırken oluşan hataların ve zafiyetlerin sonradan yapılan güncellemeler ile ortadan kaldırılmasıdır.

- Yama Yönetim (Patch Management) : Yazılımları güncel tutmak ve güvenlik risklerini bertaraf etmek amacıyla yamaların alınması, test edilmesi ve uygulanması süreçlerini kapsayan sistemler yönetimidir.

- Yanıltma (Spoofing) : Siber saldırgan veya suçluların, bir hedef ip adresine kendini başka bir ip adresindenmiş gibi gösterip bağlanması işlemine denir.

- Yemleme : Bu saldırı türünde siber saldırganlar şans ilkesi temelinde hedef şahıslara e-postalar gönderirler. Bu e-postlar, hedef şahsın dikkatini çekecek şekilde sanki bir e-posta veya internet hizmeti sağlayıcısından gönderilmiş gibi tasarlanır. Bu e-postalarda hedef şahsa kredi kartı şifresi, hesap bilgisi, e-posta veya sosyal medya hesabı ile ilgili sahte güncelleme taleplerinin olduğu bir başka web sitesine yönlendirilen URL bağlantısı yer alır.

- Yetkilendirme (Authorization) : Bir kurum tarafından hangi kaynaklara hangi kullanıcıların erişim sağlayabileceğini tespit eden süreçtir.

- Yetkisiz Erişim (Unauthorized Access) : Kullanma yetkisi verilmediği halde herhangi bir sisteme, ağa veya kaynağa izinsiz erişim yapma işlemidir.

Z

- Zafiyet (Vulnerability) : Bilgisayar programları yazılırken yanlışlıkla yapılan kodlama hatalarıdır.

- Zafiyet Analizi (Vulnerability Analysis) : Zafiyetlerin tanımlanması ve sınıflandırılması sürecidir.

- Zararlı Reklam Yazılımı (Adware) : Bilgisayarlarda reklamlar görüntülemek, arama isteklerini reklam web sitelerine yeniden yönlendirmek ve özelleştirilmiş reklamların görüntülenmesi için ziyaret edilen web sitelerinin türleri gibi kullanıcılara dair pazarlama verilerini toplamak amacıyla tasarlanmış programlara verilen addır.

- Zararlı Yazılım (Malware) : Kullanıcı tarafından izin verilmeyen işlemleri gerçekleştiren kötü amaçlı programlardır. Bilgisayar virüsü, solucan, casus yazılım, adware, truva atı, Botnet şeklinde tasnif edilebilirler.

- Zorunlu Erişim Kontrolü (Mandatory Access Control / MAC) : Bir kurum bünyesinde erişim haklarının kurallar ve prensipler dahilinde sürdürülmesidir.