VERİ GÜVENLİĞİ

Avrupa Ekonomik Topluluğu 1983'te Bilişim Suçları konusunda şu tanımlamayı yapmış ve günümüzde birçok ülke bu tanımlamayı esas almıştır. **Bilişim suçu;** bilgileri otomatik olarak işleme tabi tutan veya verilerin nakline yarayan bir sisteme karşı veya sistem ile gayri kanuni, ahlak dışı ve yetkisiz gerçekleştirilen he türlü davranıştır.

- **Phreaker:** Telefon ağları üzerinde çalışan, telefon sistemlerini hackleyerek bedava görüşme yapmaya çalışan kişilerdir.
- **Script kiddie:** Script kiddie'ler hacker'lığa özenen kişilerdir. Tam anlamıyla hacker değillerdir. Script kiddieler genellikle kişilerin e-posta veya anında mesajlaşma şifrelerini çalarlar.
- **Lamer:** Ne yaptığının tam olarak farkında olmayan, bilgisayar korsanlığı yapabilmek için yeterince bilgisi olmayan kişilerdir.

- Bilişim sistemi bilgi ve verinin bilgisayar desteği ile yönetilmesi demektir. Bilişim sistemleri hayatın her alanında olduğu gibi güvenlik sistemleri alanında da kullanılmaktadır. Bilgisayarlar, hayatımızın her alanında kullanılmasından dolayı güvenlik sistemlerinin de bir parçası olmuşlardır.
- Bilgisayarlar herhangi bir güvenlik sistemi için basit bir ekran görevi göreceği gibi bir bankada güvenliği sağlayan sunucu olarak da kullanılabilir.
- Bilgisayar ve Bilişim Güvenliği sistemlerinde üç ana bileşenden bahsedebilir. Bu temel bileşenler donanım, yazılım ve insandır. İnternetin yaygınlaşmasıyla bu bileşenlere ağlar (internet/intranet) eklenmiştir.

Siber Suçlular

Bilişim alanında, siber tehdidin nedeni bilgisayar korsanı (hacker) olarak adlandırılan kişilerdir. Bilgisayar korsanı, şahsî bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişilerdir

Kişisel ilgi, intikam, eğlence veya şöhret gibi farklı sebeplerle motive olabilmektedirler. Artan teknoloji ile beraber bilgisayar korsanlarının türleri de değişmektedir. Bunlardan bazıları:

- **Beyaz Şapkalı (White-hat) bilgisayar korsanları:** Kötü amaçlı bilgisayar korsanlarına karşı sistemin koruyucusu gibi davranırlar. Amaçları, veriyi güvende tutmak ve her türlü çatlağı doldurmaktır.

Bilgisayar korsanları bilişim sistemine zarar vermek için değişik yollar deneyerek sistemlere saldırı yapan kişilerdir. Bu kişileri özelliklerine göre aşağıdaki gruplara ayırabiliriz.

- **Amatörler:** Bunlar genelde saldırıları eğlence için yapan kişilerdir. Sisteme zarar vermek amacı gütmeyen bu saldırganların tek amacı, sistemdeki açıklıkları tespit ederek, bu açıklıklardan faydalanmaktır. Bu gruba giren kötü niyetli kişiler genellikle reşit olmayan veya henüz reşit olmuş kişilerdir. Sistemlerdeki açıklıklardan faydalanarak arkadaş grupları arasında eğlenmek isterler. Çoğu zaman yaptıkları saldırıların nasıl sonuçlar doğuracağını bilmezler. Tüm zamanların en ünlü 10 siber suçluları arasında yer alan Jonathan James 16 yaşında tutuklanmıştır.

- Teknolojik değişimlerin son derece hızlı olduğu bir devirde yaşamaktayız. Geçen yüzyılın başlarından itibaren artan teknolojik gelişmeler, bu yüzyılda daha hızlı bir şekilde gelişme göstermiştir. 21.yüzyılda yaşamı en fazla etkileyen faktörlerden biri teknoloji haline gelmiştir.
- Teknolojinin ve bu teknolojilerin kullanımının artmasına paralel olarak bilişim sistemlerine yönelik işlenen suçlar da artmaktadır. Teknolojinin gelişmesiyle ortaya çıkan suç türlerinden birisi siber suçtur. Sibernetik kökeninden gelen ve İngilizce karşılığı "cyber" olan siber sözcüğü, bilgisayar ağlarına ait olan anlamındadır. Yani siber, sanal olanı ifade etmektedir.
- Siber Suç, bir bilişim sisteminin güvenliğini ve/veya kullanıcısını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber Suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bilgisayar ve internete özgü suçlar olarak da adlandırılabilir

- **Siyah Şapkalı (Black-hat) bilgisayar korsanları:** Yasadışı bir işlemden kişisel çıkar elde etmek isteyen kötü niyetli kişilerdir. Sistem erişim yetkisi çalarlar, kişisel bilgileri kopyalarlar veya sistemleri kırarlar.
- **Gri şapkalı (Grey hat) bilgisayar korsanları:** Bunlar beyaz şapka ve şapka korsanları arasındadır. Yeni başlayanlara yönelik bir bilgisayar korsanı olarak adlandırılabilirler. Hem iyi hem de kötü niyetleri olabilir, ancak çoğunlukla bu hackerlar eğlenmek veya kendilerini test etmek için hareket ederler.
- **Yazılım korsanı:** Yazılım korsanları bilgisayar programlarının kopya korumalarını kırarak, bu programları izinsiz olarak dağıtımına olanak sağlayıp para kazanırlar. Piyasaya korsan oyun ve program CD'lerini yazılım korsanları çıkarır.

- **Kıncılar (hacker):** Bilişim sistemine girmeye çalışan kişilerdir. Amaçları sisteme zarar verip, değerli bilgi ve belge elde etmektir. Amatörlere göre daha bilinçli hareket ederler. Belli bir amaç doğrultusunda saldırılarını gerçekleştirirler. Bu kişiler saldırılarının nasıl sonuçlar doğuracağını bilir ve ona göre hareket ederler. Çoğu zaman amaçları para elde etmek olsa da daha çok şifre kırmayı başardıklarını ve bir bilişim sistemine saldırı gerçekleştirebildiklerini göstermek isterler.
- **Kariyer Suçluları:** Amatör ve hackerlardan farklı olarak kariyer suçluları belli bir hedefe odaklanmış kötü niyetli kişilerdir. Amaçları ne eğlence ne de paradır. Asıl amaçları idealleri doğrultusunda terör ortamı oluşturmak, kargaşa yaratmak, siyasi kriz ve benzeri ciddi sonuçlar doğuracak ortamlar oluşturmaktır. Belli bir siyasi, terör veya dini örgüte üyedirler. Örgüt hedefleri doğrultusunda hareket ederler. Yaptıkları saldırılar çok önemli sonuçlar doğurabilir.

Siber suçlular genellikle Derin Web (deep web) olarak adlandırılan özel internet ağlarından yararlanırlar. Derin Web internetin çıktığı ilk tarihlerden itibaren arama motorlarının endeksleyemediği verilerin bulunduğu bilgileri içeren binlerce linkten oluşan bir sistemdir. İnternet siteleri çeşitli nedenlerden görüntülenmemek isteyebilir. Örneğin; kütüphane arşivleri, kamu ve özel şirket bilgileri gibi Genellikle herkes tarafından görülmesi istenmeyen veya İndekslenmeleri zor olan içerik Taşıdıkları için arama Motorlarında görüntülenmek istemezler. Arama linki verilmeyen veya arama motorları tarafından bulunamayan bütün siteler Derin Ağ'dan ulaşılabilir

Donanım Saldırıları

Bilgisayar donanımı, bir bilgisayarı oluşturan fiziksel parçaların genel adıdır. Bilişim sistemlerinde donanım olarak adlandırdığımız parçalar bilgisayar kasası, ekran, klavye, fare, ağ kabloları, bilgisayar kasası içerisindeki ana kart, işlemci, hafıza ve buna benzer somut nesnelerdir.
Donanımlar iç ve dış donanımlar olmak üzere ikiye ayrılırlar.

•Dış donanım (Harici Donanım) bağımsız kasa, kutu veya kılıf içinde bulunan bilgisayar kasası içinde yer almayan donanımlardır.

• İç donanım (Dahili Donanım) bir donanım parçası, başka bir donanım parçası içine yerleştiriliyorsa dahili donanım olarak adlandırılır. Başka bir değişle kasa içinde bulunan donanımlar dâhili donanım olarak adlandırılır. Bunlara örnek olarak kamera, USB girişi, Bluetooth, kızılötesi tarayıcı, yazıcı ve benzeri verilebilir.

Yazılım ve Ağ Saldırıları

Yazılımlara karşı yapılabilecek saldırılar şunlardır:

• Yazılımlar başka bir yazılımla yer değiştirilebilir.
• Yazılımların içeriği değiştirilebilir
• Yazılımlar tamamen yok edilebilir.
• Yazılımlar olması gereken yerden başka yerlere yüklenebilir.
• Yazılımlar çalınabilir.
• Başkalarına ait olan yazılımlar izinsiz kopyalanabilir.

BİLİŞİM SALDIRILARI

Bilişim sistemlerine karşı gerçekleştirilebilecek saldırılar işletmenin zafiyetleri sonucunda meydana gelir. İşletme zafiyetlerini tespit eden kişiler çeşitli araçlar kullanarak bu zafiyetleri kullanır ve sisteme sızabilir. Bilişim sistemlerine karşı gerçekleştirilebilecek saldırılar değişik parametrelere göre sınıflandırıp açıklanabilir. Tehditleri genel özelliklerine göre aşağıdaki gibi dört ana gruba ayırabiliriz.

• Ele geçirme: Kötü niyetli kişilerin veya yetkisiz kişilerin erişim yetkisi hakkı olmadıkları her türlü bilgi, belge ve varlığı değişik yöntemler kullanarak elde etmeleridir.

Donanım fiziksel veya somut parçalardan oluşur. Bu nedenle hem güvenlik görevlileri hem de kötü niyetli kişiler sisteme bağlı olan donanım parçalarını kolaylıkla görebilir.

Donanıma karşı yapılabilecek saldırılar aşağıdaki gibi sıralanabilir:

• Yeni parça eklenebilir veya parça çıkarılabilir.
• Donanım parçaları üzerine işlevlerini engelleyecek şekilde değişik sıvılar dökülebilir.
• Ağ kabloları kesilebilir.
• Donanım bileşenleri çalınabilir.
• Elle veya değişik kesici aletlerle donanımlara zarar verilebilir.
• Elektronik bilgi ve belgelerin saklandığı cihazlara (sabit diskler, harici sabit diskler, flaş bellekler, CD'ler, DVD'ler vb.) zarar verilebilir.

Yazılımlara karşı yapılan çoğu saldırı fark edilemeyecek değişikliklere yol açar. Görünüşte yazılım normal olarak çalışıyor görünür. Fakat ön tarafta normal çalışıyor görünen program arka tarafta başka amaç için çalışıyor olabilir. Donanıma karşı yapılacak saldırılara göre yazılımlara karşı olan saldırıları tespit etmek daha zordur.

CTRL+ALT+DELETE tuşlarına basın ve Görev Yöneticisi'ne tıklayarak bilgisayarınızdaki arka planda çalışan programları görebilirsiniz. Yazılımlara karşı yapılacak saldırılarda ana amaç yazılımların değiştirilmesidir. Kötü amaçlı yazılımların isimleri amaçlarına yönelik olarak tarih, biyoloji gibi gündelik hayatta insanların kolayca anlamlandırabileceği kelimelerden seçilmiştir.

• Sekteye uğratma: Kötü niyetli kişiler bilişim sistemine ait herhangi bir parçayı sekteye uğratırlar. Ele geçirme saldırılarında belgelerin kopyası yapılır veya haberleşme dinlenir. *Sekteye uğratma saldırılarında* ise belgenin aslı çalınır veya haberleşme kesilir. Belge veya mesajın karşı tarafa ulaşması engellenir.

• Değişiklik: Herhangi bir değerli varlığın içeriğinin değiştirilmesidir. Örneğin elektronik posta yoluyla haberleşen iki kişi arasındaki mesajın içeriğinin değiştirilerek karşı tarafa gönderilmesi bu tür bir saldırıdır. Özellikle yazılım parçalarının içeriğinin değiştirilmesi için yapılan saldırılar bu gruba dâhildir.

• Fabrikasyon: Sahte nesnelerin yapılmasıdır. Güvenlik odalarına girerken yetkili kişilerin kimlik doğrulama için kullandıkları kimlik kartlarının sahtelerinin yapılması bu tür saldırıdır. Bunun yanında sahte internet sitelerine yönlendirerek şifre bilgilerinin çalınması da olabilmektedir.

Yazılım ve Ağ Saldırıları

Yazılım çeşitli görevler yapma amaçlı tasarlanmış elektronik aygıtların, birbirleriyle haberleşebilmesini ve uyumunu sağlamak amaçlı makine komutlarıdır.

Bilgisayar sistemlerinde yazılımlar iki ana gruptan oluşur. Bunlar sistem yazılımları ve uygulama yazılımlarıdır.

Sistem yazılımlarına örnek M.S. Windows işletim sistemidir. Uygulama yazılımlarına örnek ise M.S. Word programıdır. Bunlar kelime işlemci, işlem tabloları, elektronik posta yazılımları ve buna benzer programlardır.

Bu tür kötü amaçlı yazılımlardan en bilinenleri kısaca aşağıdaki gibi özetlenebilir:
• Virüsler: Virüs yazılımlar kötü etkilerini bir bilgisayardan diğerine bulaştırırlar. Kendini çalıştırmalı ve kendini çoğaltmalı olarak iki gruba ayrılabilirler. Bunlar geliş kaynağı belli olmayan elektronik postalara eklenmiş dosyalardan bulaşabilir. Yine güvenilirliğini bilmediğimiz internet sayfalarında değişik programları bilgisayarımıza yüklemeye çalışırken bulaşabilir.

• Solucanlar: Solucanlar, daha karmaşık yapıya sahip olan zararlı yazılımlardır. Genellikle e-posta ile gönderilen ekler, çeşitli web siteleri ve ağ üzerinde paylaşılan dosyaları kullanarak yayılırlar.

Yazılım ve Ağ Saldırıları

Truva Atları: Bu tür kötü amaçlı yazılımlar görünüşte normal bir iş yapıyor görünür ama saklanarak arka planda başka işler yaparlar.

Rootkit(Kök kullanıcı takımı): Çalışan süreçleri, dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program grubudur. Amacı yayılmak değil, bulunduğu sistemde varlığını gizlemektir.

Keylogger (Klavye dinleme sistemi): Klavyede bir harfe dokunulduğunda casus yazılım dinler ve klavye harflerini kaydeder. Kullanıcı bankacılık şifreleri, e-posta şifreleri ve yazışma içerikleri gibi önemli bilgilerin ele geçirilmesinde kullanılır.

İnsanlara Yapılan Saldırılar

Bilişim sistemlerinin en önemli bileşeni insandır. Donanım ve yazılımlar insan unsurunun karar vermesine yardımcı olması için vardır.

Bu kapsamda iyi eğitilmiş insan gücü güvenliğin sağlanmasındaki en önemli etkenlerden biridir. Kurumların teknolojinin tek başına güvenlik problemini çözebileceğini düşünmesi, güvenlik probleminin ve güvenlik teknolojilerin tam anlaşılmadığının göstergesidir.

Sosyal mühendislik; internette insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır.

Güvenlik görevlisini değişik yöntemlerle ikna ederek, kapıdan giriş yetkisi olmayan birisinin içeri girmesinin sağlanması da yine sosyal mühendisliğe örnektir.

Unutulmamalıdır ki kötü niyetli kişiler önemli kişileri veya kilit konumdaki çalışanları ikna etmek için her türlü yolu deneyebilirler.

Sosyal mühendislikte güvenlik sistemleri açısından kötü niyetli kişilerin uyguladıkları yöntemlerden bazıları aşağıdaki gibidir:

- Taklit ve inandırma
- Yetkisiz fiziksel erişim
- Klavye ile yazı yazarken çevredeki birinin sizi gözlemlemesi
- Yardım masası aramalarının taklit edilmesi
- Kimsenin olmadığı açık odalar bulabilmek için koridorda dolaşma.

- **Ransomware (Fidye yazılımı):** Fidye yazılımları bulaştığı bilişim sistemleri üzerinde dosyaları erişimi engelleyerek kullanıcılardan fidye talep eden zararlı yazılımlardır.

- **Spyware (Casus yazılım):** Casus yazılımlar kullanıcılara ait önemli bilgilerin ve kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan yazılım olarak tanımlanabilir.

- **SPAM (İstenmeyen e-posta):** İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesidir. SPAM çoğunlukla ticari reklam niteliğinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, yarı yasal servislerin duyurulması amacına yöneliktir

Bilişim sistemlerinin en önemli bileşeni insandır. Donanım ve yazılımlar insan unsurunun karar vermesine yardımcı olması için vardır.

Bu kapsamda iyi eğitilmiş insan gücü güvenliğin sağlanmasındaki en önemli etkenlerden biridir. Kurumların teknolojinin tek başına güvenlik problemini çözebileceğini düşünmesi, güvenlik probleminin ve güvenlik teknolojilerin tam anlaşılmadığının göstergesidir.

Güvenlik sistemlerinin bir parçası olarak bakıldığında insanlara yönelik yapılan en önemli saldırı sosyal mühendisliktir.

Sosyal mühendislik; internette insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır.

BİLİŞİM GÜVENLİĞİ TEDBİRLERİ

Bilişim güvenliği bilişim aygıt ve yazılımlarının kullanımından doğabilecek riskleri ve tehlikeleri inceleyen bilişim teknolojisi dalıdır.

Bilgi güvenliği yazılı, sözlü veya elektronik ortamdaki bilginin korunması ve doğru bilginin, doğru zamanda, doğru kişiye ulaştırılmasıyla ilgilenir

Hangi yöntem kullanılırsa kullanılsın %100 güvenli bir sistem elde etmek zordur. Bu anlamda güvenlik tedbirleri risk olasılıklarını azaltmak üzere faaliyetler içerir. Bu tedbirler en genel anlamıyla **önleme, tespit ve kurtarma** şeklinde ifade edilebilir.

Yazılım ve Ağ Saldırıları

Herhangi bir bina, kurum veya şirketin güvenliğinin sağlanması için kullanılan bütün güvenlik mekanizmaları (ekranlar, güvenlik kameraları, X-ray cihazları, turnikeler ve buna benzer), bu mekanizmaları kontrol eden bilgisayarlar ve diğer bilgisayarlar kablolu veya kablosuz olarak birbirine bağlanarak bir ağ oluşturur.

Günümüzde bulut sistemler sayesinde işletmelerin bilgi ve belgeleri bulut sistemlerinde tutulmaktadır.

Güvenlik görevlisini değişik yöntemlerle ikna ederek, kapıdan giriş yetkisi olmayan birisinin içeri girmesinin sağlanması da yine sosyal mühendisliğe örnektir.

Unutulmamalıdır ki kötü niyetli kişiler önemli kişileri veya kilit konumdaki çalışanları ikna etmek için her türlü yolu deneyebilirler.

Sosyal mühendislikte güvenlik sistemleri açısından kötü niyetli kişilerin uyguladıkları yöntemlerden bazıları aşağıdaki gibidir:

- Taklit ve inandırma
- Yetkisiz fiziksel erişim
- Klavye ile yazı yazarken çevredeki birinin sizi gözlemlemesi
- Yardım masası aramalarının taklit edilmesi
- Kimsenin olmadığı açık odalar bulabilmek için koridorda dolaşma.

- **Önleme:** Önleme bilişim güvenliği tedbirlerinin en önemli parçasıdır. Önleme adımının temel amacı oluşabilecek siber saldırıların engellemesidir.

Önleme adımında yapılması gerekenler, **engelleme/caydırma, saldırıyı zorlaştırma ve hedef saptırmadır.** Bir saldırının gerçekleşmesini tamamen engellemek hemen hemen imkânsızdır. Siber saldırıları tamamen engellemek çok zor olduğundan bu saldırıların gerçekleştirilmesini zorlaştırmak veya caydırmak gerekmektedir.

Alışveriş yapılabilen internet sitelerinde kullanıcılara güven vermek ve saldırganları caydırmak için alınan tedbirlerden bir bölümünün logoları konur

• **Önleme:** saldırgan işletmeye saldırı düzenlemenin zor olduğunu veya kimliğinin tespit edilip ifşa edilebileceğini düşünür.
Tamamen engellenemiyorsa, bu saldırıların gerçekleştirilmesi mümkün olduğunca zorlaştırılmalıdır.
Bazı durumlarda saldırının zorlaştırılması da mümkün olmayabilir. Bu durumda hedef saptırma yöntemi kullanılarak saldırıları asıl hedeften sahte hedeflere yönlendirmek gerekir.
Firmaya ait çok gizli bilgilerin olduğu dosyalara olacak saldırılarda, hedef saptırmak için kötü niyetli kişilerin dikkatini çekecek şekilde sahte dosyalar oluşturarak bu saldırganları bu dosyalara yönlendirmek mümkündür. Bu da yine hedef saptırma olarak kullanılacak bir yöntemdir.

BİLİŞİM GÜVENLİĞİ TEDBİRLER
İnsanlara Yönelik Tedbirler

Bilişim sistemleri güvenliği dediğimizde, genel olarak bilgisayar güvenliğinden bahsedilmektedir. Fakat güvenlik sistemlerine tehditlerin ve bu tehditlere alınan önlemlerdeki açıkların en önemli kaynağı insanlardır.

Kötü niyetli yazılımları hazırlayanlar farklı motivasyonlarla hareket edebilmektedir. Yüksek güvenirlikli yerlere kötü niyetli yazılımların bulaşmasındaki en önemli etkenin bu kurumlarda çalışan insanların bilinçli veya bilinçsiz yapmış olduğu hataların olduğu tespit edilmiştir.

Siber saldırı yöntemleri nelerdir?

• Zararlı yazılımlar,
• Hizmet dışı bırakma, (DDOS saldırıları şu anda en etkili teknolojik silahlardan biri),
• Siber casusluk,
• Sosyal mühendislik,
• Oltalama (Phishing),
• APT (Gelişmiş Kalıcı Tehditler),
• Mobil ve sosyal medya aracılığıyla yapılan saldırılar,
• Güvenlik zafiyetleri kullanılarak yapılan saldırılar

siber saldırılara örnek olarak verilebilir.
Siber saldırılarda kullanılan araçlar bakımından %25'le zararlı yazılımlar ilk sırada. %23'le DDOS atakları ikinci sırada yer alıyor. DDOS ataklarını %12'le web tabanlı ataklar, %11'le oltalama saldırıları izlemekte.

Bir siber savaşta neler tehdit altında?

Bir siber savaşta öncelikle,
• Savunma sistemleri,
• Telekomünikasyon sistemleri,
• Su ve enerji dağıtım şebekeleri,
• Ulaşım sistemleri,
• Finansal altyapılar,
• Sağlık sistemleri,
• Kamu kurumları,
• ve vatandaş
büyük tehdit altında.

• **Tespit:** Bir saldırı olduğunda ikinci aşamada yapılması gereken bu saldırıların tespit
edilmesidir. Tespit için gözlem yapılması gerekir. Tespit yapılabilmesi için "Ağ Topolojisi" olarak adlandırılan ağın tüm unsurlarını içeren liste ve haritalama olmalıdır. Ağa hareketleri sürekli izlenmeli, "Log" kayıtları gözden geçirilmelidir. Şüpheli durumlar ile ilgili sistem yöneticileri "Saldırı Tespit Sistemleri" ile uyarılmalıdır

• **Kurtarma:** Saldırıları tespit ettikten sonra bu saldırıların sistemimize verdiği zararları belirlemek gerekir ve ardından sistemi işler hale getirmek gereklidir. Bunun yanında saldırıyı gerçekleştiren kötü niyetli kişilerin tespit edilmesi ve gerekli hukuki sürecin de başlatılması gerekir.

Örneğin yüksek güvenirlikli kurumlarda çalışan insanların sıkça gittiği kafe vb. yerlerde ücretsiz dağıtılan, düşürülmüş hissi uyandıran usb belleklerin çalışanlarca alınıp kurumda kullanılması insanların oluşturduğu tehditlere örnek olarak verilebilir.

Bu ve bu gibi tehdit unsurlarının önlenmesinde insan kaynağının eğitimi oldukça önemlidir. Kurum çalışanlarına sistem güvenliği tehditleri ve tedbirlerine yönelik farkındalık eğitimleri düzenlenmeli ve bu eğitimler belirli aralıklarla tekrarlanmalıdır.
.

TEŞEKKÜRLER

BİLİŞİM GÜVENLİĞİ TEDBİRLERİ
Donanıma Yönelik Tedbirler
Donanıma karşı yapılacak saldırılardan korunmak için kullanılan en yaygın kontrol mekanizması fiziksel korunmadır.

Bu nedenle bilgisayar ve bilişim sisteminin donanımı güvenli bir alanda korunur. Bu alana giriş ve çıkışlar kontrollüdür. Güvenlik odası dediğimiz bu alan sürekli kilitli tutulmalı ve kapalı devre televizyon sistemleri ile izlenmelidir.

Bunlara ek olarak kişilerin kimliklerini doğrulamak için kullanılan her türlü cihaz da donanım bu tedbirler arasında sayılabilir. Kapı giriş sistemleri, güvenlik kartları donanıma yönelik tedbirlerden sadece bir kaçıdır.

Belge Bilgi Güvenliği Konusunda Çalışan Kurumlar
Ülkemizde bilgi belge güvenliği Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından sağlanmaktadır.

USOM ülkemizde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması adına kurulmuştur. İnternet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyon USOM vasıtasıyla gerçekleştirilmektedir.

USOM siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri yapmakta, kritik sektörlere yönelik siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlamaktadır.