BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMİ

"Kurumsal Bilgi Güvenliği Farkındalığı Programları"nı desteklemek üzere oluşturulmuş e-öğrenme eğitim içerik dokümanıdır."

Modül A – Bilgi Güvenliği Farkındalığı

Hedef Kitle : Kurum Yönetim Ekipleri, Kurum Çalışanları, Bireyler

İçerik : Temel bilgi güvenliği farkındalığı oluşturmaya yönelik olarak hazırlanmıştır. Bu modüllerin içeriği kurumlara göre özelleştirilmeyecek şekilde hazırlanmıştır.

Modül B – Kurumsal Bilgi Güvenliği Politikaları ve Uygulamaları

Hedef Kitle : Kurum çalışanları, BT Ekipleri

İçerik : Temel bilgi güvenliği farkındalığı eğitimini tamamlayan kurum çalışanları ve Bilgi Teknolojileri ekipleri için hazırlanmıştır. Bu modüllerin içeriklerinin bir bölümü kurumların politikaları ve uygulamalarına göre özelleştirilecek şekilde hazırlanmıştır.

Ek Modüller

Modül C – Oltalama Simülasyonu

Hedef Kitle : Bilgi güvenliği farkındalığı modülünü tamamlayan kurum çalışanları

Modül D - Kişisel Verilerin Korunması Kanunu Farkındalığı

Hedef Kitle : Kişisel verileri işleyen, transfer eden, barındıran ortamlara/ hizmetlere sahip kurumlardaki ilgili çalışanlar

Modül E - Kart Verisini Koruma (PCI DSS)

Hedef Kitle : Kart verileri işleyen, transfer eden, barındıran ortamlara/ hizmetlere sahip kurumlardaki ilgili çalışanlar

Modül F - Çocuklarınız için Siber Güvenlik Farkındalığı

Hedef Kitle : Internet, akıllı telefon ve/veya tablet kullanan çocukları olan kurum çalışanları

Modül G - Güvenli Yazılım Geliştirme (OWASP Top 10)

Hedef Kitle : Kurumlardaki Yazılım/Uygulama Geliştirme ekipleri

A.1 - Bilgi Güvenliği Temel Kavramları

A.1.1. Konu anlatımı:

- Bilgi Güvenliği ve Siber Güvenlik tanımları
- Temel Bilgi Güvenliği Kavramları
- Gizlilik
- Bütünlük
- Kullanılabilirlik/Erişilebilirlik
- Bilgi güvenliğinin yapı taşları
- "İnsan" : En zayıf halka mı ? en güçlü halka olabilir mi?

A.1.2. Senaryo:

Konu anlatımındaki bölüm kullanıcıların ilgisini çekecek bir senaryo işlenecektir.

A.2 - Bilgi Yaşam Döngüsü

A.2.1. Konu anlatımı:

- Understand why organizations classify their information
- Bilginin değerini belirleme çalışmaları
- Bilgi sınıflandırması çalışması
- Practice classifying information according to its level of sensitivity
- Apply best practices for handling information according to its classification level
- Learn how to safely use portable storage devices and media.
- Learn techniques for properly disposing of and destroying confidential data and files.

A.2.2. Senaryo:

Konu anlatımındaki bölüm kullanıcıların ilgisini çekecek bir senaryo işlenecektir.

A.3 - Bilgi Güvenliğine Yönelik Tehdit Kaynakları

A.3.1. Konu anlatımı:

- Dış kaynaklı tehditler
  - Bir saldırganın şirket web sayfasını hacklemesi
  - Yetkisiz bilgi ifşası, veri sızdırma
  - Şirket ağının internete açık kısımlarına yönelik DDoS saldırısı
  - Hedef odaklı karmaşık siber saldırılar

- İç kaynaklı tehditler
  - Bilinçsiz kullanım sonucu oluşabilecek riskler
    - Temizlik görevlisinin sunucunun fişini çekmesi
    - Eğitilmemiş çalışanın veri tabanını silmesi
    - Yazılım geliştiricinin örnek aldığı kod içerisinde zararlı kod çıkması (Java script, encoding)
  - Kötü Niyetli Hareketler
    - İşten çıkarılan çalışanın, kuruma ait web sitesini değiştirmesi
    - Bir çalışanının, ağda sniffer çalıştırarak E-postaları okuması
    - Bir yöneticinin, geliştirilen ürünün planını rakip kurumlara satması

A.3.2. Senaryo:

Yaşanan olaylar ve manşetlerden uygun bir müzik eşliğinde bir derleme yapılacaktır. Yurtdışı olaylar kullanılarak, olayların hangi tehditler kaynaklı oluştuğu vurgulanıp farkındalık artırılması hedeflenmektedir.

A.4 - Saldırı Kavramı ve Türleri

A.4.1. Konu anlatımı:

- DOS/DDOS (Hizmet Aksatma) saldırıları
- Ticari bilgi ve teknoloji hırsızlıkları
- Web sayfası içeriği değiştirme saldırıları (defacement)
- Virüs , worm , trojan kavramları
- Yetkisiz erişim denemeleri
- Teknolojik Casusluk
- Siber Şantaj
- Sahtekarlık ve taklit (Uygulama)

A.4.2. Senaryo:

Yaşanan olaylar ve manşetlerden uygun bir müzik eşliğinde bir derleme yapılacaktır. Yurtdışı olaylar kullanılarak, olayların hangi tehditler kaynaklı oluştuğu vurgulanıp farkındalık artırılması hedeflenmektedir.

A.5 - Sosyal Mühendislik

A.5.1. Konu anlatımı:

Sosyal Mühendislik, saldırganın kendi isteği doğrultusunda davranmanız için kandırıldığınız bir tür psikolojik saldırıdır. Dolandırma ya da kandırma düşüncesi yeni değildir, sosyal mühendislik binlerce yıldır varolmuştur. Ancak siber saldırganlar bu tekniği internette kullanmanın son derece etkili olduğunu keşfetmişler ve milyonlarca insanın bir anda hedef alınabileceğini öğrenmişlerdir. Sosyal Mühendisliğin nasıl islediğini öğrenmenin en kolay yolu, yaygın olan gerçek bir örneğe bakmaktır.

Internet Servis Sağlayıcınız ya da kullandığınız işletim sisteminin teknik destek hizmetleri gibi bilgisayar destek hizmetlerinden olduğunu iddia eden bir kişiden telefon alırsınız. Arayan kişiler, bilgisayarınızın garip davrandığını tespit ettiklerini, örneğin bilgisayarınızın interneti taradığını ya da istenmeyen e-posta (spam) gönderdiğini, ve bilgisayarınıza virüs bulaşmış olduğunu düşündüklerini belirtirler. Bu sorunu araştırmak ve bilgisayarınızı daha güvenli hale getirmek için iş basındadırlar. Bir sürü teknik terim kullanırlar ve bilgisayarınıza virüs bulaşmış olduğuna sizi ikna etmek için kafa karıştırıcı adımlardan bahsederler.

Örneğin, bazı dosyaların bilgisayarınızda olup olmadığını kontrol etmenizi isteyebilir ve sizi bu dosyaları nerede bulacağınız konusunda yönlendirebilirler. Bu dosyaları bulduğunuzda telefondaki kişi, bu dosyaların sizin bilgisayarınıza virüs bulaştığının bir göstergesi olduğuna sizi ikna edecektir ki aslında bu dosyalar her bilgisayarda bulunan yaygın sistem dosyalarından başka birşey değildir. Bilgisayarınıza virüs bulaştığı konusunda sizi oyuna getirince, bir ağ sitesinden onların güvenlik yazılımını alma konusunda size baskı yapacak ya da bilgisayarınızı onarmak için uzaktan erişimi vermenizi isteyeceklerdir. Ancak onların sattıkları program aslında kotü niyetli bir yazılımdır. Eğer alırsanız ve yazılımı yüklerseniz sadece kandırılmakla kalmayacak bir de bunu yapmaları için onlara para ödemiş olacaksınız. Eğer uzaktan erişim hakkını verirseniz, gerçekte onlar virüs bulaştırarak bilgisayarınızı ele geçireceklerdir.

Unutmayın, bunun gibi sosyal mühendislik saldırıları sadece telefon konuşmaları ile sınırlı değildir. E-posta, kısa mesaj, Facebook mesajları, Twitter bildirimleri ya da çevrim-içi sohbetlerini kullanarak yapılan otalama saldırıları dahil hemen hemen her teknoloji ile mümkün olabilir.

Sosyal Mühendislik Saldırılarını Belirlemek ve Durdurmak

Sosyal Mühendislik saldırılarına karşı savunmanın en kolay yolu sağduyunuzu kullanmaktır. Eğer bir şey şüpheli görünüyorsa ya da ters giden bir şey varmış gibi geliyorsa o zaman bu bir saldırı olabilir. Sosyal mühendislik saldırıları aşağıdaki gibi bazı ortak işaretler taşır:

- Birisi aşırı derece aciliyet hissi yaratıyorsa. Eğer kendinizi hızlı bir karar verme noktasında buluyorsanız, şüpheci davranın.
- Birisi ulaşmaması gereken bir bilgi soruyorsa ya da zaten önceden bilmesi gereken
- İnanılmayacak derecede iyi bir şey olmuşsa. Kuraya katılmamanıza rağmen kazandığınız konusunda bilgilendirilmeniz bu durum için bilinen yaygın bir örnektir.

Eğer birinin sizi sosyal mühendislik saldırısının kurbanı yapmaya çalıştığından şüpheleniyorsanız, o kişi ile bir daha asla iletişim kurmayın. Eğer bu telefondaki kişi ise, kapatın. Eğer çevrim-içi sohbette ise, bağlantınızı kapatın. Eğer güvenmediğiniz bir yerden gelen bir mail ise, silin. Eğer işle ilgili bir saldırı ise, iş yerindeki yardım masasına ya da bilgi güvenliği takımına haber verin.

Gelecekteki Olası Saldırıları Engellemek

Neyse ki gelecekteki olası saldırılara maruz kalmanızı engellemenize yardımcı olacak önlemler vardır.

- **Şifrelerinizi Asla Paylaşmayın**. Hiçbir kurum şifrenizi sormak için sizinle iletişime geçmez. Eğer biri size şifrenizi soruyorsa bu bir saldırıdır.
- **Çok Fazla Bilgi Paylaşmayın**. Bir saldırgan sizin hakkınızda ne kadar çok bilgiye sahipse sizi o kadar kolay bulup istedikleri şeyi yaptırmak için yanlış yönlendirebilir. Zaman içinde küçük bile olsa kendinizle ilgili paylaşımlarınız, hayatınızın bütünü hakkında bilgi sahibi olmak için bir araya getirilebilir. Ne kadar az bilgi paylaşırsanız, ürün eleştiri, forumlar, e-posta listeleri ya da sosyal medya siteleri dahil, o kadar az saldırıya uğrarsınız.
- **İrtibatta bulunduğunuz kişileri doğrulayın**. Zaman zaman bankanızdan, kredi kartı şirketinden, mobil servis sağlayıcınızdan ya da başka bir organizasyondan yasal gerekçelerle aranabilirsiniz. Eğer bilgi isteğinin yasal olup olmadığı hakkında herhangi bir şüpheniz varsa arayan kişinin adını ve ona ulaşabileceğiniz bir numarayı isteyin. Güvenilir bir kaynaktan şirketin telefon numarasını bulun, örneğin kredi kartınızın arkasında bulunan numaradan, hesap özetinizde yazan numaradan ya da şirketin ağ sayfasında bulunan telefon numarasından (tarayıcınıza URL'i sizin yazdığınızdan emin olun). Böylece şirketi aradığınızda gerçekten şirket personeli ile konuştuğunuzdan emin olursunuz. Bu biraz uğraştırma gerektirse de kimliğiniz ve kişisel bilgilerinizi korumak bu ek adıma değerdir.

A.5.2. Senaryo:

444 0 … - X Bankası Çağrı Merkezinden aradığını ifade eden saldırgan ile kurban arasında geçen konuşmaları konu alan bir çekim yapılabilir. Telefonla ulaşılan kişiyi, internetten ele geçirdiği bilgilerle, çağrı merkezinden aradığına ikna eden kişi, panik havası oluşturup, kurbanın kişisel bilgileri ve şifrelerini ele geçirir. Kurban durumu anladığında iş işten geçmiştir.

A.6 - Otalama

A.6.1. Konu anlatımı:

Otalama e-posta ya da mesajlaşma servislerini kullanarak sizin örneğin bir sosyal medya sitesinde bir aksiyon almanızı, bir bağlantıyı tıklamanızı ya da bir ekli dosyayı açmanızı sağlayarak sizi kandıran bir saldırı türüdür. Böyle bir saldırının kurbanı olarak riskiniz hassas bilgilerinizin çalınması ya da bilgisayarınızın ele geçirilmesi olabilir. Saldırganlar oltalama e-postalarının ikna edici olması için gerçekten çok çalışıyorlar. E-postalarını sizin tanıdığınız biri ya da bildiğiniz bir yerden, örneğin bir arkadaş ya da sıkça kullandığınız güvenilir bir şirketten geliyormuş gibi gösteriyorlar. Hatta bankanızın logolarını ekleyip, mesajın gerçekliğine sizi inandırabilmek için e-posta adreslerini onlarınkine benzetiyorlar. Sonra bu oltalama e-postalarını milyonlarca insana gönderiyorlar. Kimin tuzağa düşeceğini bilmiyorlar, tek bildikleri ne kadar çok gönderirlerse, başarma seanslarının o kadar yüksek olduğu. Otalama bir ağ̆ ile balık yakalamaya çalışmaya benzer, ne yakalayacağınızı bilemezsiniz ama ağınız ne kadar büyükse, daha fazla balık yakalama şansınız daha yüksektir. Otalama ile istediklerini elde edebilmek için saldırganların kullandıkları temel birkaç yöntem var:

Bilgi Toplama: Saldırganın amacı parolalarınız, kredi kartı ya da bankacılık bilgileriniz gibi kişisel bilgilerinizi ele geçirmektir. Bunu yapmak için size içeriğinde bilinen ve orijinal görünen bir siteye yönlendirme bağlantısı bulunan bir e-posta gönderir. Bu site sizden kişisel bilgilerinizi ya da hesap bilgilerinizi ister. Ne yazık ki bu site sahtedir ve verdiğiniz herhangi bir bilgi doğrudan saldırgana gider.

Kötü̈ Niyetli Bağlantılar: Saldırganın amacı cihazınızı kontrol altına almaktır. Bunu yapmak için size bir bağlantı içeren e-posta gönderir. Eğer bağlantıyı tıklarsanız, cihazınıza yönelik saldırı başlatan ve başarılı olursa sisteminizi ele geçiren bir siteye yönlendirilirsiniz.

Kötü̈ Niyetli Dosya Ekleri: Saldırganın amacı aynıdır, cihazınızı ele geçirmek. Ancak bir bağlantı göndermek yerine, size Word dokümanı gibi kotü niyetli bir dosya eki gönderir. Eki açmak, saldırıyı başlatır ve sisteminizi muhtemelen saldırganın ele geçirmesine yol açar.

Aldatmacalar: Bazı saldırganlar dijital hayata geçiş yapan dolandırıcılardan başka birileri değildir. Sizi bir piyango kazandığınızı söyleyerek, hayırsever bir kurum gibi yardım isteyerek ya da milyonlarca doların transferine yardımcı olmanızı isteyerek kandırmaya çalışırlar. Eğer herhangi birine yanıt verirseniz, paranızı alabilmek için sizden öncelikle hizmetleri için bir ödeme ya da banka hesap bilgilerinize erişim talep edeceklerdir.

Kendinizi / Kurumunuzu Korumak İçin

Bir e-postanın saldırı olup olmadığını anlamak için bazı ipuçları vardır, en yaygın olanlarını şöyle sıralayabiliriz:

- E-posta aciliyet hissi uyandırır, kotü birşeyler (banka hesabınızın kapatılması gibi) olmadan önce acil aksiyon almanızı ister. Saldırgan, size düşünmeden hata yapmaya zorlamak istiyordur.
- Beklemediğiniz bir dosya içeren bir e-posta alırsınız ya da e-posta size ekli dosyayı açmak için kandırmaya çalışıyordur. Henüz duyurulmamış işten çıkarmalar listesi, çalışan maaş artış bilgileri ya da hakkınızda bir dava açıldığını belirten ekler bunlara örnek olabilir.
- Sizin adınızı kullanmak yerine “Değerli Müşterimiz” gibi daha genel ifadeler kullanılır. Birçok firma ya da arkadaşlarınızın birçoğu adınızı bilir.
- Böyle e-postalar sizden kredi kartı numaranız ya da parolanız gibi yüksek hassasiyetli bilgiler ister.
- E-posta size resmi bir kurumdan geldiğini söylüyordur, ancak yazım dili hatalarla doludur ya da gönderen e-posta adresi @gmail.com, @yahoo.com, ya da @hotmail.com gibi kişisel bir hesaptır.
- Bağlantılar gariptir ya da olması gereken adresler değildir. İpucu, bağlantının üzerine gelip, gerçekte size hangi bağlantıya yönlendireceğini görerek, karar vermenizdir. Eğer görünen bağlantı ismi ile gerçekte size yönlendireceği bağlantı aynı değilse, sakın tıklamayın. Mobil cihazlarınızda bir bağlantının üzerinde parmağınızı aşağıya doğru kaydırarak bu bilgiyi görebilirsiniz. Hatta daha güvenli bir yöntem, e-postanızdaki bağlantı adresini kopyalayıp, internet tarayıcınıza yapıştırmak ya da doğru bağlantıyı yazmaktır.
- Mesaj bildiğiniz birisinden geliyordur, ancak tarz, kullandığı kelimeler ondan farklıdır. Eğer şüpheleniyorsanız, gönderen kişiyi arayıp doğrulayın. Bir siber saldırgan için kişisel ya da iş arkadaşınızdan geliyormuş gibi görünen bir e-posta oluşturmak çok kolaydır.

Eğer bir e-postanın ya da mesajın otalama saldırısı olduğuna inanıyorsanız, basitçe silin. Sağduyunuz kesinlikle en güçlü savunmanızdır.

A.6.2. Senaryo:

Saldırganlar, hedef olarak oldukça saygın bir kurumu seçerler. Linkedin üzerinden seçtikleri kurum çalışanlarını listelerler. Kurum içerisindeki sunucularda yetkileri olabileceğini düşündükleri birkaç Bilgi Teknolojileri çalışanını kurban olarak seçerler. Seçtikleri kurbanların sosyal medya hesaplarında yaptığı paylaşımları inceleyerek, hangi takımı tuttuklarını, ilgi alanlarını, vb. incelerler ve her birine özel birer otalama e-postası hazırlarlar. Yoğun bir Cuma günü akşam çıkış saatine yakın bir zamanda gönderirler ve kurbanlardan en az birinin otalama e-postasını tıklayıp açmalarını beklerler. Sonuç : Başarırlar. Kurbanlardan biri tuttuğu takımın resmi sayfasından geliyormuş gibi gösterilen bir otalama e-postasında verilen linki açar ve kazandığı bileti almak için sahte sayfada yer alan tüm soruları yanıtlar (e-postasını doğrular ve şifresini girer). Bundan sonra olacakları saldırganlar yönetecektir.

A.7 – Zararlı / Kötü Amaçlı Yazılımlar

A.7.1. Konu anlatımı:

Zararlı/kotü amaçlı yazılım (malware), basitçe bir program, kotü niyetli eylemleri gerçekleştiren yazılımlardır. Hatta İngilizcede “malware” terimi, “malicious” ve “software” kelimelerinin birleşimi ile oluşturulmuştur. Siber suçlular, kotü amaçlı yazılımı kontrolü̈ ele geçirmek veya içindeki bilgilere ulaşmak için sizin bilgisayarınız ya da cihazlarınıza kurarlar. Bir kere yüklendikten sonra bu saldırganlar kotü amaçlı yazılımı çevrim-içi işlemlerinizi gözetlemek, şifrelerinizi ya da dosyalarınız çalmak veya sizin sisteminizi kullanarak diğerlerine saldırmak için kullanırlar. Hatta kotü amaçlı yazılımlar, kendi dosyalarınıza erişiminizi engelleyerek bu dosyalara tekrar erişmek için saldırgana fidye ödeme yapmanızı bile talep edebilir.

Birçok kişi kotü amaçlı yazılımın sadece Windows yüklü̈ bilgisayarların bir problemi olduğu yanılgısını taşımaktadır. Windows yaygın bir kullanıma sahip iken, kotü amaçlı yazılımlar Mac bilgisayarlar, akıllı telefonlar ya da tabletler gibi her cihaza bulaşabilir. Siber suçlular ne kadar çok bilgisayar ve cihaza kotü amaçlı yazılımı bulaştırırlarsa o kadar çok para kazanırlar. Bu yüzden siz dahil herkes hedeftir.

Kötü̈ amaçlı yazılım artık sadece meraklı hobiciler ya da amatör korsanlar tarafından değil, tecrübeli siber suçlar tarafından yazılmaktadır. Amaçları, belki sizden çaldıkları verileri satarak, spam e-postalar göndererek, hizmeti engelleme saldırıları (denial of service attacks) yaparak ya da şantaj yaparak bulaştırdıkları bilgisayar ya da cihazlardan para kazanmaktır. Kötü̈ amaçlı yazılımları yazan, dağıtan ve bundan yarar sağlayan kişiler, kendi kendine hareket eden kişiler ile iyi örgütlenmiş suçlu grupları arasında dağılım gösterir. Komplike kotü amaçlı yazılımları yazanlar çoğunlukla bu işe kendilerini adamışlar, tam zamanlı olarak bu tip yazılımları geliştirmektedirler. Ayrıca, bir kez kotü amaçlı yazılımı yazdıklarında çoğunlukla bunu diğer kişilere veya organizasyonlara satarlar. Hatta “müşterilerine” düzenli olarak güncelleme ve destek sağlayarak.

Kendinizi/Kurumunuzu Korumak İçin

- Siber suçlular, çoğunlukla bilgisayar ve tabletlerde yüklü yazılımların açıklarından yararlanarak cihazlarınıza kotü amaçlı yazılımı bulaştırırlar. Ne kadar güncel bir sisteminiz var ise sisteminizde o kadar az açık bulunmaktadır ki bu da siber suçluların kotü amaçlı yazılımı bulaştırmalarını zorlaştırır. Bu yüzden işletim sisteminizin, uygulamalarınızın ve cihazlarınızın güncellemeleri otomatik olarak yüklemelerinin etkin olduğundan emin olun.
- Sibel suçluların mobil cihazlarınıza kotü yazılım bulaştırmada kullandıkları bilindik yol, sahte bir uygulama yaratıktan sonra internete koyarak insanların bu programı indirmesi ve yüklemesi için kandırmaktır. Bu yüzden sadece güvenilir çevrim-içi mağazalardan uygulama indirin ve yükleyin. Ayrıca sadece uzun zaman önce internete yüklenmiş, büyük bir kitle tarafından yüklenmiş ve birçok olumlu değerlendirmesi olan mobil uygulamaları indirin.
- Bilgisayarlarda “yönetici” ya da “kök (root)” hesapları gibi ayrıcalıklı bir hesap yerine limitli hakları olan standart bir hesap kullanın. Bu birçok kotü amaçlı yazılımın kendini yüklemesini engelleyerek ek bir koruma sağlayacaktır.
- Siber suçlular genellikle insanları onların yerine kotü amaçlı yazılımları yüklemeleri için kandırırlar. Örneğin, görünüşte geçerli, bir eki ya da bağlantı içeren bir e-posta gönderirler. Belki de bu e-posta bankanızdan ya da arkadaşınızdan geliyormuş gibi görünebilir. Ancak eğer ekli dosyayı açarsanız ya da bağlantıyı tıklarsanız, kotü amaçlı yazılımın yüklenmesini tetikleyen kodu aktive etmiş olursunuz. Eğer bir mesaj güçlü bir aciliyet hissi yaratıyorsa, kafa karıştırıcıysa ya da fazlasıyla iyiyse, o zaman bu bir saldırı olabilir. Şüpheci olun, sağduyu genelde sizin en iyi savunmanızdır.
- Düzenli olarak sisteminizi, dosyalarınızı bulut tabanlı servislere yedekleyin ya da yedeklerinizi örneğin harici bellek kullanarak çevrim-dışı saklayın. Bu, kötü amaçlı yazılımların dosyalarınızı şifreleme ya da silme girişimleri durumunda yedeklerinizi korumanızı sağlayacaktır. Yedeklemeler kritiktir ve çoğunlukla kötü yazılımların bulaşma durumlarından kurtulmanın tek yoludur.

Sonuç olarak, kötü amaçlı yazılımlara karşı kendinizi savunmanın en iyi yolu, yazılımları güncel tutmak, iyi bilinen sağlayıcılardan güvenilir anti-virüs yazılımları yüklemek ve sisteminize kötü amaçlı yazılım bulaştırmak için herhangibirinin sizi kandırabileceği konusunda alarm durumunda olmaktır.

A.7.2. Senaryo:

Saldırganlar, hedef olarak oldukça saygın bir teknoloji şirketini seçerler. Google'da yaptıkları bir arama ile prezentabl görünümlü, ciddi bir iş kadını fotoğrafı bulur ve bir ad/soyad uydururlar. Bu fotoğraf ve isimle bir e-posta adresi alıp, LinkedIn üzerinde iyi bilinen bir İnsan Kaynakları şirketinde çalışıyormuş gibi görünen, oldukça deneyimli ve "Senior HR Executive" ünvanıyla bir profil oluştururlar. Bu hesaptan, LinkedIn üzerinde tanımlı tüm "Senior IT Executive / Manager" pozisyonlarına "mevcut/olası BT yönetim pozisyonlarında değerlendirilmek üzere bağlantı kurmak isteyen" davetler gönderirler. Daveti alan kişilerin neredeyse tamamı, kabul eder. Aradan 1 ay geçmiştir ve 500+ bağlantıya sahip oldukça tanınan bir HR Executive profiline sahip olmuşlardır. Artık saldırı zamanı gelir. Hedef aldıkları teknoloji şirketinin halihazırda bağlantı davetlerini kabul eden çalışanlarına bir zero-day açıklığı kullanan bir Word dosyası ileterek, içeriğindeki bilgileri doldurmalarını isterler. Tabii, acele algısı oluşturup mesai saatleri içinde ve internete bağlı kurum bilgisayarlarından doldurmalarını zorlayarak. Sonuç : Başarırlar. Kurbanlardan biri zararlı yazılım içeren dosyayı açar, internetten indirilen yazılım, önce onun bilgisayarına, sonra da ağda bulunan ve kurbanın yetkisi olan diğer ortamlara bulaşır. Bundan sonra olacakları saldırganlar yönetecektir.

A.8 – Sosyal Medya ve Bilgi Güvenliği

A.8.1. Konu anlatımı:

Sosyal medya ile ilgili genel kaygı kişisel bilgilerin korunmasıdır. **Potansiyel tehlikeler şunlardır:**

Geleceğinizin etkilenmesi: Bazı kuruluşlar özgeçmiş kontrolü için sosyal medya platformlarını kullanmaktadır. Utandırıcı veya suç içeren fotoğraflar veya gönderiler, ne kadar eski olursa olsun, işe alınmanızı veya terfi etmenizi engelleyebilir. Ayrıca, bazı üniversiteler de aynı araştırmaları öğrenci kabul süreçlerinde yapmaktadır. Bu kuruluşlar, sizden sayfalarını "beğenmelerini" veya sayfalarına katılmanızı isteyebileceği veya bazı gönderiler birden fazla sitede arşivlenebileceği için gizlilik ayarları sizi korumayabilir.

Size karşı saldırılar: Siber saldırganlar gönderilerinizi analiz ederek, bu bilgileri size veya sizin kuruluşunuza ait bilgilere erişim sağlamak için kullanabilir. Örneğin, saldırganlar paylaştığınız bilgileri; parolanızı sıfırlamak için kullanılan "gizli soru"larınızın cevaplarını tahmin etmek için, hedef odaklı e-posta oltalama saldırıları yapmak için veya siz gibi davranıp kuruluşunuzdaki birisini telefonla aramak için kullanabilir. Ayrıca, bu ataklar çalıştığınız veya yaşadığınız yerin öğrenilmesi gibi fiziksel dünyayı da etkileyebilir.

İşvereninize yanlışlıkla zarar vermek: Suçlular veya rakipler, kuruluşunuz ile ilgili paylaştığınız her türlü hassas bilgiyi işvereninize karşı kullanabilir. Ayrıca, gönderileriniz kuruluşunuzun saygınlığına zarar verebilir. İşiniz ile ilgili herhangi bir paylaşım yapmadan önce, kuruluşunuzun politikalarını kontrol ettiğinizden ve sosyal medya hesaplarınızın izlenmediğinden emin olun.

En iyi koruma yöntemi, paylaşımlarınızı sınırlamaktır. Gizlilik ayarları bir miktar koruma sağlayabilir, ancak, bu özellikler genelde karışıktır ve sizin bilginiz olmadan çok sık değişir. Gizli olduğunu düşündüğünüz bir şey, çeşitli sebepler nedeniyle bir anda genele açık olabilir. Ayrıca, gönderilerinizin gizliliği insanların onu paylaştığı kadar güvendedir. Bilgiyi ne kadar arkadaşınız veya kişi ile paylaşırsanız, o kadar genele açık olacaktır. Paylaştığınız herhangi bir şeyin genele açık bir hale geleceğinin veya gelebileceğinin ve o paylaşımın internet'in kalıcı bir parçası olacağının veya olabileceğinin farkında olmalısınız.

Son olarak, arkadaşlarınızın sizinle ilgili paylaşımlarına dikkat etmelisiniz. Sizi rahatsız eden bir şey paylaştıklarında, onlardan bu paylaşımı kaldırmasını isteyin. Eğer, bu isteğinizi reddederlerse, sosyal medya platformu ile irtibata geçerek kaldırılmasını istemelisiniz. Aynı zamanda, siz de başkaları ile ilgili yaptığınız paylaşımlarda saygılı olmalı ve dikkat etmelisiniz.

Güvenlik

Gizlilik başlığı altındaki önerilere ek olarak bu başlık altında da sosyal medya hesaplarınız ve çevrimiçi aktivitelerinizi korumak için bazı adımlar bulunmaktadır.

Giriş: Tüm hesaplarınızı güçlü, benzersiz parola ile korumalı ve bu parolayı kimseyle paylaşmamalısınız. Ayrıca, bir çok sosyal medya platformu iki aşamalı doğrulama gibi güçlü kimlik doğrulama yöntemlerini desteklemektedir. Mümkün olan her zaman bu güçlü kimlik doğrulama yöntemleri etkinleştirilmelidir. Son olarak, sosyal medya hesaplarınızı başka internet sitelerine giriş için kullanmayın; eğer hesabınız ele geçirilirse bütün hesaplarınız savunmasız kalacaktır.

Gizlilik Ayarları: Gizlilik ayarlarını kullanıyorsanız, bu ayarları iyi inceleyin ve düzenli olarak test edin. Sosyal medya platformları sık sık gizlilik ayarlarını değiştirdikleri için hata yapmak kolaydır. Ayrıca, bir çok uygulama ve servis konum bilgisi eklemenize imkan tanır (bu özellik geotag olarak adlandırılır). Eğer konum bilginizin gizli kalmasını istiyorsanız, bu ayarları düzenli olarak kontrol edin.

Şifreleme: Sosyal medya platformları çevirimiçi bağlantılarınızı koruyan ve HTTPS olarak adlandırılan şifrelemeyi kullanır. Twitter ve Google+ gibi platformlar bu şifreleme yöntemini varsayılan olarak kullanırken, diğer platformlarda manuel olarak etkinleştirilmesi gerekmektedir. Sosyal medya hesabınızın ayarlarını kontrol edip varsayılan bağlantı olarak HTTPS şifrelemesini etkinleştirin.

E-posta: Sosyal medya platformlarından gelmiş gibi gözüken şüpheli e-postalara dikkat edin, bu e-postalar siber suçlular tarafından gönderilen aldatıcı saldırılar olabilir. Bu tip mesajlara cevap vermenin en güvenli yolu, muhtemelen kaydedilmiş bir yer iminden doğrudan sosyal medya platformuna giriş yapmak ve mesajları okumak veya cevap vermektir.

Zararlı bağlantılar/'Scam': Sosyal medya platformlarında bulunan şüpheli bağlantılar ve potansiyel 'scam'lar (dolandırıcılık faaliyetlerinde bulunan internet siteleri) konusunda dikkatli olun. Art niyetli kişiler, saldırılarının yayılması için sosyal medya platformlarını kullanır. Arkadaşınız tarafından gönderilen bir ileti, gerçekten ondan geldiği anlamına gelmez; hesabı ele geçirilmiş olabilir. Bir aile üyesi veya arkadaşınız doğrulayamayacağınız

garip bir mesaj gönderirse (örneğin, soyulduğunu söylüyor ve sizden para istiyorsa), onlara telefonla veya mesajın ondan geldiğini doğrulayabileceğiniz başka bir yöntemle ulaşın.

Mobil Uygulamalar: Sosyal medya platformlarının çoğu çevirimiçi hesaplarınıza erişmeniz için mobil uygulamalar sağlar. Bu mobil uygulamaları güvenilir kaynaklardan indirdiğinizden ve akıllı telefonunuzun güçlü bir parola ile korunduğundan emin olun. Akıllı telefonunuzu kaybettiğinizde kilitli değilse, herhangi biri sosyal medya hesaplarınıza erişerek sizin yerinize paylaşımlar yapabilir.

Sosyal medya platformları, dünyanın geri kalanıyla iletişim kurmak ve bağlantıda kalmak için harika bir yoldur. Burada özetlediğimiz ipuçlarını takip ederseniz, çok daha güvenli çevrimiçi deneyimi yaşayabilirsiniz. Sosyal medya platformlarını güvenli kullanmak ve yetkisiz faaliyetleri bildirmek ile ilgili daha fazla şey öğrenmek için sosyal medya platformlarının güvenlik sayfalarını inceleyebilirsiniz.

- *Sosyal Ağlar üzerindeki uygulamalar (aplikasyonlar) ve izinleri*
- *Sahte marka ve sahte ünlü hesapları*
- *Sosyal ağlar üzerine yüklediğiniz fotoğraflar*
- *Sosyal ağlar üzerindeki açıklıklar*
- *Sosyal ağ yöneticilerinin hacklenmesi ve hesap güvenliği*
- *Sosyal medya ajansları ve yöneticilerinin güvenlik bilinci*
- *Fotoğraflar ve meta data bilgileri*
- *Fotoğraflar ve GPS bilgileri*
- *Fotoğraflar ve Stenografi ile bilgi paylaşımı*
- *Ip adresiniz ve yer tespiti*
- *Paylaşımlarınızdan kişilik tahlili*
- *Paylaşımlarınız içerisindeki hakaretler*
- *Yalan haber ve sahte haber paylaşımları*

A.8.2. Senaryo :

Sosyal ağlarla ilgili senaryo işlenecektir.

A.9 - İletişim Sistemleri ve Bilgi Güvenliği

A.9.1. Konu anlatımı:

İletişim aracı olarak e-posta kullanırken birey olarak dikkat etmeniz gerekenler;

Otomatik Tamamlama: Otomatik tamamlama birçok e-posta uygulamasında bulunan genel bir özelliktir. E-posta göndermek istediğiniz kişinin adını yazmaya başladığınızda, e-posta uygulamanız otomatik olarak onun e-posta adresini sizin için seçer. Bu yöntemle, tüm kontaklarınızın e-posta adreslerini hatırlamak zorunda kalmazsınız, sadece alıcının adını hatırlamanız yeterlidir. Otomatik tamamlama konusundaki problem, benzer isimlere sahip birden çok kontağınız olduğunda ortaya çıkar. Otomatik tamamlamanın sizin için yanlış e-posta adresini seçmesi çok kolaydır. Örneğin, şirketinizin Muhasebe bölümünde çalışan arkadaşınız "Ali Yılmaz"e tüm finansal bilgilerinizi içeren bir e-posta göndermek niyetindesiniz. Ancak bunun yerine otomatik tamamlama özelliği komşunuz "Ali Yılmazel"i seçebilir ve sonuçta yetkisi olmayan kişilere hassas bilgileri göndermiş olabilirsiniz. Kendinizi buna karşı korumak için "gönder" tuşuna basmadan önce daima ismi ve e-posta adresini iki kez kontrol edin.

Dağıtım Listeleri: Dağıtım listeleri tek bir e-posta adresi ile temsil e-posta adreslerinin toplamıdır, bazen posta listesi veya grup adı olarak adlandırılır. Örneğin, e-posta adresi group@example.com olan bir dağıtım listeniz olabilir. O adrese bir e-posta gönderdiğinizde, mesaj gruptaki herkese, belki yüzlerce ya da hatta binlerce kişiye iletilir. Bir dağıtım listesine e-posta gönderirken çok dikkatli olun çünkü birçok insan bu mesajı alabilir. Ek olarak bir kişinin bir dağıtım listesine gönderdiğI e-postayı yanıtlarken, çok dikkatli olun. Sizin sadece bireysel olarak göndereni yanıtlama niyetiniz olabilir, ama "Tümünü Yanıtla" seçeneğini tıkladığınızda, bu özel yanıtınız o listedeki yüzlerce hatta binlerce insan tarafından okunuyor olacaktır. Otomatik tamamlama bir dağıtım listesini seçerken de tehlikeli olabilir. Sizin niyetiniz, örneğin çalışma arkadaşınız Carl'a (carl@example.com adresine) bir e-posta göndermek iken, otomatik tamamlama yanlışlıkla arabalar hakkında abone olduğunuz bir dağıtım listesine (car@example2.com) gönderebilir.

Mahremiyet (Kişisel Gizlilik): Geleneksel e-posta uygulamalarında çok az gizlilik koruma yöntemi olduğunu hatırlayın, e-postanız ona erişen herkes tarafından okunabilir. Buna ek olarak, bir telefon veya kişisel görüşmenin aksine, bir e-postayı gönderdiğinizde artık bunun üzerinde hiçbir kontrolünüz kalmaz. E-postanız kolayca başkalarına iletilebilir, halka açık forumlarda yayınlanabilir, ve sonsuza kadar internette erişilebilir kalabilir. Eğer iletişim kurmak için gerçekten hassas bir konunuz varsa, telefon açın. Birçok ülkede, e-postaların mahkemelerde delil olarak kullanılabilir olduğunu hatırlamanız da önemlidir. Son olarak eğer e-posta göndermek için iş bilgisayarınızı kullanıyorsanız, işvereninizin sizin e-postalarınızı izlemek ve hatta belki de okumak için hakkı olabileceğini unutmayın. Hatta kişisel e-posta hesabınıza erişmek için iş bilgisayarınızı kullanıyorsanız, bu hak, kişisel e-postalarınızı da içerebilir.

- *Tüm bilişim güvenliğimiz e-postaya bağlıdır, nasıl?*
- *E-posta ve internet iletişimi altyapısı nasıl çalışır, yönlendirilir?*
- *Snowden dünyasında iletişim güvenliği ve bireysel mahremiyet*
- *E-posta ve mesajlaşma güvenliği*
- *E-postanın kim tarafından kime gönderildiği nasıl belirlenir?*
- *Temel E-posta güvenlik politikaları*
- *E-postalar spamdan nasıl korunur?*
- *Sahte/Taklit E-postalar ve çalışma mantığı*
- *PKI(Gizli/Açık anahtar altyapısı) çalışma yapısı*
- *Güvenli e-posta kullanımı için öneriler*
- *Mail güvenliğinde PKI kullanımı ve güvenlik getirileri*
- *Webmail programlarında SSL kullanımı ve Two factor authentication*
- *Bulut ortamında tutulan e-postaların güvenliği*
- *Popüler mesajlaşma programları ve şifreleme*
- *Tango, Line, Viber, WhatsUp ve Skype yazılımları*
- *Mesajlaşma yazılımları ve gizlilik*

A.9.2. Senaryo:

Güvenli e-posta kullanımı için önerileri, slayt olarak anlatılarak bunların nasıl uygulandığını gösteren bir video gösterilecektir.

A.10 - Mobil Sistemler ve Bilgi Güvenliği

A.10.1. Konu anlatımı:

Mobil sistemlerde güvenliği sağlamak için İlk adım her zaman emin olduğunuz, güvenilir bir kaynaktan indirmektir. Herhangi birinin bir mobil uygulama geliştirebileceğini hatırlayın, dolayısıyla onları nereden edindiğiniz konusunda çok dikkatli olmalısınız. Siber suçlular gerçeğinden ayırdedilemeyen ve kötü niyetli yazılımlar içeren uygulamalar yaratma ve dağıtmadaki becerilerini çok geliştirdirler. Eğer bu uygulamalardan birini kurduysanız, bu suçlular e-postalarınızı okumak, konuşmalarınızı dinlemek ya da kontaktlarınızın bilgilerini almak için mobil cihazınızın kontrolünü ele geçirebilirler. Uygulamaları sadece iyi bilinen, güvenilir kaynaklardan indirerek, kötü niyetle değiştirilmiş uygulamaları kurma ihtimalinizi azaltırsınız. Bu konuda farkında olmadığınız şey, seçeneklerinize kullandığınız mobil cihazın markasının karar vermesi olabilir.

iPad ya da iPhone gibi Apple cihazlarında, mobil uygulamaları sadece Apple “app store” adı verilen yönetilen bir ortamdan indirebilirsiniz. Bunun avantajı, Apple’ın hem mobil uygulamalar hem de yazarları ile ilgili güvenlik kontrolü yapmasıdır. Apple tüm kötü niyetli insanları ya da yazılımları yakalayamıyor olsa da, bu yönetilen ortam kötü niyetli bir yazılımı indirme riskini çok büyük bir oranda azaltır. Buna ek olarak, eğer Apple böyle bir yazılımı bulursa, hızlı bir şekilde “app store” dan kaldırmaktadır. Windows Phone da, uygulamaları yönetmek için buna benzer bir yaklaşım kullanır.

Android mobil cihazlar farklıdır. Android size internet üzerinde istediğiniz yerden mobil bir uygulamayı indirme esnekliği verir. Ancak bu esneklik, aynı zamanda daha fazla sorumluluk

demektir. İndirip kurduğunuz mobil uygulamaların tamamı gözden geçirilmediğinden çok daha dikkatli olmanız gerekir. Google, adı "Google Play" olan ve Apple'ınkine benzeyen bir yönetilen mobil uygulama dükkanına sahiptir. Google Play'den indirdiğiniz uygulamalar bazı temel kontrollerden geçmektedir. Bu nedenle biz sizlere, Android cihazlarınız için uygulamaları, Google Play'den indirmenizi öneriyoruz. Diğer internet sitelerinden Android mobil uygulamaları indirmekten kaçının zira herhangi bir siber suçlu çok basit bir şekilde bir kötü niyetli uygulama yaratıp dağıtabilir. Ek bir koruma önlemi olarak, mobil cihazınıza anti-virüs yazılımı kurmayı değerlendirin.

Riski daha da azaltmak için, çok yeni olan, sadece birkaç kişinin indirdiği ya da çok az olumlu yorum almış uygulamalardan uzak durun. Bir uygulama ne kadar uzun süredir yayındaysa ya da ne kadar çok olumlu yorum aldıysa, o kadar güvenilir olmaya yakındır. Ek olarak sadece ihtiyacınız olan ve kullanacağınız uygulamaları indirin. Kendinize, bu uygulamaya gerçekten ihtiyacım var mı diye sorun. Her uygulama yeni potansiyel güvenlik açıklıkları getirebileceği gibi, aynı zamanda kişisel bilgi gizliliği konuları da oluşacaktır. Eğer bir uygulamayı kullanmaktan vazgeçtiyseniz, mobil cihazınızdan silin (eğer ihtiyaç duyarsanız her zaman yeniden ekleyebilirsiniz) Son olarak, mobil cihazınızı jailbreak ya da root yapmış olabilirsiniz. Bu, cihazınızın mevcut özelliklerini değiştirme ve onaylanmamış uygulamaları yükleyebilme sürecidir. Biz bunu sadece birçok güvenlik kontrolünü atlattığınız için değil aynı zamanda garanti ve destek sözleşmelerinizi de geçersiz kıldığı için hiç önermiyoruz.

İzinler: Bir mobil uygulamayı güvenilir bir kaynaktan kurduktan sonraki aşama, güvenli bir şekilde konfigüre edilmesi ve sizin kişisel bilgilerinizin gizliliğinin korunmasıdır.Mobil uygulamaları kurmak ve / veya konfigüre etmek genel olarak belirli izinlerin verilmesini gerektirir. Bir uygulamaya herhangi bir izni vermeden once mutlaka bu uygulamanın işini yapabilmesi için gerçekten bunlara ihtiyacı var mı diye düşünün. Örneğin, bazı uygulamalar konumlandırma servislerini kullanır. Eğer bir uygulamaya bu izni verirseniz, bu uygulamanın yaratıcısına tüm hareketlerinizi izleme hakkı verirsiniz, hatta başkalarına bile satabilirler. Eğer bir uygulamaya, sizden istediği izinleri vermek istemiyorsanız, uygulama dükkanında ihtiyacınızı karşılayan başka uygulama seçenekleri olup olmadını araştırın. Apple cihazları lokasyon bilgisine erişim gibi bazı izinleri "Ayarlar" seçeneğinden değiştirmenize izin verir. Windows ve Android mobil cihazları farklıdır, size ya hep, ya hiç yaklaşımını sunar. Eğer bir uygulamanın istediği tüm izinleri vermezseniz, uygulamayı kuramazsınız.

Uygulamaları Güncellemek: Mobil uygulamalar, tıpkı bilgisayarınız ve mobil cihazınızın işletim sistemi gibi güncel kalabilmeleri için güncellenmelidir. Suçlular sürekli bir şekilde uygulamalardaki açıklıkları aramak ve bulmak ile meşgul. Sonrasında da bu açıklıkları kullanan saldırılar geliştiriyorlar. Uygulamalarınızı yazanlar da, bu açıklıkları kapatan ve cihazlarını koruyan güncellemeler yayınlıyorlar. Güncellemeleri ne kadar sık kontrol edip kurarsanız, o kadar iyidir. Birçok platform mobil uygulamalarınızın güncellemelerini otomatik olarak kontrol etmenize izin veriyor. Biz bu seçeneği kullanmanızı öneriyoruz. Bu mümkün değilse, en azından her iki haftada bir uygulamalarınızın güncelliğini kontrol etmenizi öneriyoruz. Bununla birlikte her güncelleme sonrasında uygulamalarınızın yeni izinlere gereksinimi olup olmadığını doğruladığınızdan emin olun.

- *GPS bilgilerini kayıt eden işletim sistemleri*
- *GPS bilgisi kullanan uygulamalar*
- *Telefonunuzu uzaktan yöneten uygulamalar*
- *Mobil işletim sistemleri açıklıkları*
- *Uygulama marketlerinde kredi kartı kullanımı*
- *Bluetooth ve üzerinden gelen virüsler*
- *SMS ve MMS üzerinden gelen virüsler*
- *Telefonunuzu ses kayıt cihazına dönüştüren uygulamalar*
- ~~*IOS JB ve Android root erişimi sağlamanın zararları*~~
- *MDM(Mobile Device Management) çözümleri*

A.10.2. Senaryo:

Telefonun kamerasını ve mikrofonunu kullanma izni isteyen bir oyunun, kurumsal bir telefona indirilmesi ve sonrasında önemli bir ihale/toplantı sırasında yapılan dinleme/izlemenin kurumu zarara uğratması konusu aktarılacaktır.

A.11 - Seyahatler ve Bilgi Güvenliği

A.11.1. Konu anlatımı:

Ev ya da işyerindeki ağınız güvenli olabilir ancak yolculuk yaparken bağlandığınız herhangi bir ağın güvenilmez olduğunu varsaymak zorundasınız. Kimlerin bu ağda olduğunu ve hangi tehditleri yaratacağını bilemezsiniz. Yolculuk yaparken bilgilerinizi korumak için birkaç basit ön kontrol ölçütü size çok yardımcı olabilir. Yolculuğa çıkmadan bir ya da iki hafta önce:

- Yanınızda götüreceğiniz cihazlarınızda hangi bilgilere ihtiyacınız olmadığını belirleyin ve gereksiz bilgileri kaldırın. Bu, eğer cihazınızı kaybeder, çaldırır veya cihazınıza sınır görevlisi ya da gümrük tarafından el konulursa önemli ölçüde olumsuz etkiyi azaltmanıza yarayacaktır. Eğer bir iş gezisi ise danışmanlarınıza şirketin yolculukta kullanabileceğiniz olası başka bir cihaz temin edip edemeyeceğini sorun.
- Uluslararası yolculuklar için, gideceğiniz ülkenin hangi tip elektrik bağlantısı kullandığını öğrenin, cihazlarınızı şarj etmek için adaptör kullanmak zorunda kalabilirsiniz. Dahası, mobil servis sağlayıcınızın size seyahatte iken hangi servisleri sunduğunu kontrol edin. Genel olarak mobil servis sağlayıcıları uluslararası kullanımı daha fazla ücretlendirirler. Hücresel veri kabiliyetinizi kapatmayı ya da uluslararası tarifenizi değiştirmeyi isteyebilirsiniz.
- Cihazınız çalındığında ya da kaybettiğinizde uzaktan cihazınızın nerede olduğunu takip etmek ve hatta uzaktan içindeki bilgileri silmek için bir yazılım yükleyin. Birçok mobil cihaz bu özelliği ile birlikte gelir, yapmanız gereken sadece bunu etkinleştirmenizdir. (Unutmayın, bu programlar çalışmak için internet erişimine ihtiyaç duyar.)

Yolculuğa çıkmadan bir ya da iki gün önce:

- Son versiyonlarını kullandığınızdan emin olmak için cihazlarınızı, uygulamalarınızı ve anti-virüs yazılımlarınızı güncelleyin.
- Cihazınızdaki tüm uygun güvenlik ayarlarını etkinleştirin, güvenlik duvarı gibi.
- Tüm mobil cihazlarınızı güçlü bir şifre ile kilitleyin. Bu yolla, eğer cihazınızı kaybeder ya da çaldırırsanız, insanların sizin bilgilerinize ulaşmasını engellersiniz.
- Verilere ulaşılmasını engellemek için tüm cihazlarınızı şifreleyin. iPhone gibi bazı cihazlar, bir şifre tanımladığınızda bunu otomatik olarak yapmaktadır.
- Tüm cihazlarınızı baştan sona yedekleyin. Bu yolla, eğer siz seyahatte iken cihazlarınızın başına herhangi birşey gelse bile güvenli bir yerde duran tüm verilerinize ulaşabilirsiniz.

Kaybolan/Çalınan Cihazlar: Gezinize başladığınızda fiziksel olarak cihazlarınızın emniyette olduğundan emin olun. Örneğin, hiçbir zaman cihazlarınızı arabada insanların görebileceği bir yerde bırakmayın çünkü hırsızlar arabanın camını kolayca kırarak değerli olan herşeyi alabilirler. Bir çözüm, dizüstü bilgisayarınız gibi cihazlarınızı fiziksel olarak kilitlemek için yanınızda kablo götürmenizdir. Eğer suç işlenmesi tamamen bir risk unsuru ise farkına varamayacağınız şey cihazınızı kaybetmenizin çaldırmanızdan daha olası olduğudur. Verizon'un on yıllık araştırmasına göre, insanların cihazlarınızı kaybetme olasılıkları, çaldırma olasılıklarından 15 kat daha fazla. Bu da seyahat sırasında, örneğin havaalanında güvenlikten geçerken, taksi, restoran ya da otel odasından ayrılırken veya uçaktan inerken, cihazınızı iki kez kontrol etmeniz gerek demek oluyor.

Wi-Fi Erişimi: Seyahat ederken internete erişmek çoğu zaman otelde, kafelerde ya da havalanında ortak kullanılan Wi-Fi erişim noktalarını kullanmak demek oluyor. Ortak kullanılan Wi-Fi erişim noktalarının problemi sadece bu ağı kimin kurduğunu bilmemeniz değil, kimin bu ağa bağlandığını bilememeniz. Hal böyle olunca bu noktalar güvenilmez olarak algılanmalı, hatta yolculuğa çıkmadan tüm önlemleri almanızın nedeni bu. Ayrıca, Wi-Fi radio frekanslarını kullanarak sizin cihazınızla iletişime geçer, bu da size fiziksel olarak yakın olan herhangi birinin potansiyel olarak bu iletişime ulaşabileceği ve dinleyebileceği anlamına gelir.

Bu sebeple ortak kullanılan bir Wi-Fi'ye bağlanıyorsanız, tüm çevrim-içi aktivitelerinizin şifreli olduğundan emin olun. Örneğin, tarayıcınız ile çevrim-içi işlem yapıyorsanız ziyaret ettiğiniz ağ sitelerinin şifreli iletişimi desteklediğinden emin olun (URL'lerinde 'https://' ve kapalı bir asma kilit simgesi vardır). Bununla birlikte, tüm çevrim-içi aktivitelerinizin şifrelendiği VPN (Sanal Özel Ağ) hesabına sahip olabilirsiniz. Bu size şirketiniz tarafından verilmiş ya da kendi kullanımınız için bu özelliği almış olabilirsiniz. Eğer güvenebileceğiniz hiçbir Wi-Fi erişim noktası yok ise, mobil telefonunuza bağlanmayı düşünebilirsiniz (Uyarı: Daha önceden de belirtildiği gibi, uluslararası seyahat yaparken pahalı olabilir, mobil servis sağlayıcınızdan kontrol edin.)

Ortak Kullanıma Açık Bilgisayarlar: Otel lobilerinde, kütüphanelerinde ya da internet kafelerde kullanılan ortak kullanıma açık bilgisayarları kullanmayın. Sizden önce kimlerin kullandığı hakkında hiçbir bilginiz yoktur ve bu ortak kullanılan bilgisayara isteyerek ya da istemeyerek virus bulaştırmış olabilirler. Mümkün olan her yerde çevrim-içi aktivitelerinizde sadece kontrol edebileceğiniz ve güvendiğiniz bilgisayarları kullanın. Eğer ortak kullanılan bir bilgisayarı kullanmak zorunda iseniz giriş yapılacak ya da şifre girilecek hiçbir servis kullanmayın.

A.11.2. Senaryo:

Otel ücretsiz ağına benzer bir isimle yayın yapan bir saldırganın, tuzağına düşenlerin bilgilerini nasıl ele geçirdiğine dair bir video olacaktır.

A.12 - Temel Korunma Yöntemleri

A.12.1. Konu anlatımı:

Teknoloji hayatımızda giderek daha fazla önem kazandıkça karmaşıklığı da artmakta. Teknolojinin ne kadar hızlı değiştiğI göz önüne alındığında güvenlik önerileriyle başa çıkmak da kafa karıştırıcı olabiliyor. Sanki her zaman ne yapıp ne yapmayacağınızla ilgili yeni bir öğüt olacakmış gibi görünüyor. Ancak nasıl güvende olacağınız hakkında detaylar zamanla değişse bile kendinizi korumak için her zaman yapabileceğiniz temel şeyler var. Kullandığınız teknolojiden ya da kullanım yerinizden bağımsız olarak size şunları öneriyoruz:

1. Siz: Başta ve öncelikle bilmelisiniz ki tek başına teknoloji sizi koruyamaz. Saldırganlar güvenlik teknolojilerinin çoğunu atlatmanın en kolay yolunun size saldırmak olduğunu öğrendiler. Eğer sizin şifrenizi ya da kredi kartı bilgilerinizi istiyorlarsa onlar için bunun en kolay yolu sizi oyuna getirerek bu bilgileri sizden almaktır. Örneğin, sizi Microsoft teknik hizmet personeli gibiymiş gibi arayabilir ve bilgisayarınıza virus bulaştığını öne sürebilirler ki gerçekte bu kişiler siber suçlular olup istedikleri, bilgisayarınıza erişmek için gerekli bilgileri edinmektir. Ya da belki de size paketinizin teslim edilemediğine dair bir e-posta atacaklar ve adresinizi teyit etmek için bir bağlantıyı takip etmenizi isteyeceklerdir ki gerçekte sizin kötü niyetli bir ağ sitesini ziyaret etmenizi sağlayarak bilgisayarınıza izinsiz bir şekilde gireceklerdir. Sonuçta saldırganlara karşı en büyük savunmanız kendinizsiniz. Şüpheci olun, sağduyunuzu kullanarak birçok saldırıyı fark edebilir ve durdurabilirsiniz.

2. Güncelleme: Bilgisayarınızın, mobil cihazlarınızın, uygulamalarınızın ve ağınıza bağlı herşeyin üzerinde son versiyon yazılımların kurulu olduğundan ve çalıştığından emin olun. Siber suçlular sürekli olarak kullandığınız teknolojilerin zayıf noktalarını bulmaya çalışırlar. Bir zafiyet yakaladıklarında bu zayıf noktaları kullanarak hangi teknolojiyi kullanıyorsanız ona izinsiz girmeye çalışırlar; ağınız, bilgisayarınız ve mobil cihazlarınız dahil. Eş zamanlı olarak sizin kullandığınız teknolojiyi geliştiren şirketler de yazılımları güncel tutmak için sıkı çalışırlar. Bir zayıf nokta ortaya çıktığında, bu zayıf noktayı onarmak için bir yama ortaya çıkarır ve genel kullanım için yayınlarlar. Siz ise bilgisayar ve mobil cihazlarınızın bu güncellemeleri yaptığından emin olarak, bilinen zayıf noktaları azaltıp izinsiz girişleri daha zor hale getirirsiniz. Güncel kalmak için her fırsatta otomatik güncellemeyi etkinleştirin. Bu kural ağa bağlı herhangi bir teknoloji için geçerlidir; internete bağlı televizyonlar, bebek monitörleri, ana yönlendiriciler (home router), oyun konsolları ya da belki bir gün arabanız. Eğer

bilgisayarınızın işletim sistemi, mobil cihazınız ya da kullandığınız başka herhangi bir teknoloji artık desteklenmiyor ve artık herhangi bir güncelleme almayacak ise desteklenen yeni bir sürüme geçmenizi öneriyoruz.

3. Parolalar: Kendinizi korumak için bir sonraki adım, herbir cihazınız, çevrim-içi hesabınız ve uygulamalarınız için güçlü ve eşsiz parolalar kullanmayı gerektirir. Buradaki anahtar kelimeler güçlü ve eşsiz'dir. Güçlü bir parola, bilgisayar korsanları ya da onların otomatik araçları tarafından kolayca tahmin edilemeyecek olan bir parola demektir. Yalnız bir kelime yerine sembol ve rakamları ek olarak içeren birden fazla kelimeden oluşan uzun bir parola kullanın. Eşsiz ise her bir cihazınız ve çevrim-içi hesabınız için ayrı bir parola kullanmanız demektir. Bu yolla eğer bir parolanız ele geçirilirse, diğer hesaplarınız ve cihazlarınız hala güvende olacaktır. Güçlü ve eşsiz parolalarınızı hatırlayamıyor musunuz? Üzülmeyin biz de hatırlayamıyoruz. İşte bu yüzden size, tüm parolalarınızı şifreli bir formatta güvenli bir şekilde saklayan, bilgisayarınız ya da mobil cihazınız için özel bir yazılım olan parola yöneticilerini tavsiye ediyoruz. Son olarak eğer hesaplarınızdan herhangi biri iki aşamalı doğrulamayı destekliyorsa her zaman bu özelliği etkinleştirmenizi tavsiye ediyoruz çünkü bu hesabınızı korumanın en güçlü yollarından biridir.

4. Şifreleme: Size tavsiye edeceğimiz diğer bir adım şifrelemeyi kullanmaktır. Şifreleme, sadece siz ya da sizin güvenebileceğiniz kişilerin bilgilerinize ulaştığından emin olmanızı sağlar. Veri iki yerde şifrelenir: hareketsiz ya da hareketli iken. Hareketsiz iken verilerin şifrelenmesi, verilerin dosya olarak sabit diskinizde ya da USB çubuğunuzda saklanıyor iken korunması anlamına gelir. Bir çok işletim sistemi, Tüm Disk Şifreleme (Full Disk Encryption) gibi özellikleri kullanarak bütün verilerinizi otomatik olarak sifrelemenize olanak verir. Her fırsatta bunu etkinleştirmenizi öneririz. Hareketli veriyi şifrelemek ise verinizin bilgisayarınızdan ya da cihazınızdan diğer cihazlara aktarılması sırasında şifrelenmesi anlamına gelir; örneğin çevrim-içi bankacılık işlemleri yaparken. Doğrulama yapmanın en kolay yolu, şifreleme etkin ise ziyaret ettiğiniz ağ sitesinin adresinin "https" ile başladığından ve kapalı asma kilit imgesinin adresin yanında bulunduğundan emin olmaktır.

5. Yedekleme: Bazen ne kadar da dikkatli olursanız olun, cihazlarınız ya da hesaplarınızdan biri ele geçebilir. Eğer durum buysa genellikle tek seçenek, bilgisayarınızın ya da mobil cihazınızın kötü amaçlı yazılımlardan arındığından emin olduktan sonra baştan yapılandırmaktır. Saldırgan kişisel dosyalara, resimlere ve diğer bilgilerinize ulaşımınızı engellemiş bile olabilir. Sizin tek seçeneğiniz ise yedeklemelerinizi kullanarak tüm kişisel bilgilerinizi geri yüklemek olabilir. Düzenli olarak önemli bilgilerinizin yedeklemelerini yaptığınızdan emin olun ve bu bilgilerin geri yüklenebilieceğini doğrulayın. Birçok işletim sistemi ve mobil cihaz otomatik yedeklemeyi desteklemektedir.

A.12.2. Senaryo:

Beş önerinin slayt gösterisi ve kısa örneklerinin olduğu bir anlatım yapılacaktır.

Modül B – Kurumsal Bilgi Güvenliği Politikaları ve Uygulamaları

- Neden kurumsal bilgi güvenliği ?
  - Bilgi teknolojilerinin kötüye kullanımı sonucu oluşan zararlar
  - Bilgiler başkalarının eline geçebilir
  - Kurumun onuru, toplumdaki imajı zarar görebilir
  - Donanım, yazılım, veri ve kurum çalışanları zarar görebilir
  - Önemli veriye zamanında erişememek
  - Parasal kayıplar
  - Vakit kayıpları
- Bilgi sızıntısı ve korunma yolları
- Genel kavramlar ve parola güvenliği
  - İyi ve kötü şifre örnekleri
  - Şifrelerin güvenli olarak muhafazası
- Yazılım Yükleme / Güncelleme ve Donanım Yönetimi
  - Güvenilir olmayan sitelerden yazılımlar indirilmemeli ve kullanılmamalıdır
- Donanım Ekleme
- İnternet'e erişim için kurum tarafından kabul edilmiş yöntemler kullanılmalıdır.
  - Bilgisayarlara modem takılmamalıdır.
  - Bluetooth ve 3G modemler ile İnternet bağlantısı yapılmamalıdır
  - 3G modem ile birlikte yerel ağı internete açmış olunuyor. 3G modem Güvenlik duvarı olmadan kullanılmamalı.
- Güvenli diz üstü bilgisayar kullanımı
- Çalınmalara karşı fiziksel güvenlik
  - ~~Parola güvenliği.~~
- BİOS parolası koruması, dik şifreleme
- Taşınabilir medya güvenliği
- Ziyaret ve ziyaretçi yönetimi / Ofis içi dolaşım sisteminde uyulması gereken kurallar
- Müşteri gizliliği / Müşteri bilgilerine verilmesi gereken önem
- Kimlik Kartının önemi / Misafir Yönetiminde Kimlik Kartı ve Yönetimi
- Dosya Erişim ve Paylaşımı
- Cloud tabanlı dosya paylaşım programları için şifreleme
- Axcrypt ve TrueCrypt şifreleme programları ile güvenli dosya paylaşımı

B.1 - Kurumsal Bilgi Güvenliği Politikası

Kurumun bilgi güvenliği politikası, bilgi güvenliği hedefleri, vb. kuruma özel bilgilerle oluşturulacak

B.2 - Kabul Edilebilir Kullanım / Internet / Sosyal Medya Kullanım Politikası

Kurumun kabul edilebilir kullanım politikası, internet ve sosyal medya kulllanım politikası, vb. kuruma özel bilgilerle ve Modül B girişte yer alan bilgilerle oluşturulacak.

B.3 – Parolalar

B.3.1 – Konu Anlatımı:

Parolaları her gün, e-posta hesabınıza erişmekten çevrimiçi bankacılığa kadar, çevrimiçi alışverişten akıllı telefonunuza erişmeye kadar bir çok noktada kullanırsınız. Oysa, parolalar sizin en zayıf noktalarınızdan biridir. Birisi sizin parolanızı öğrenirse kimliğinizi çalabilir, paranızı transfer edebilir veya kişisel bilgilerinize erişebilir. Güçlü parolalar, kendinizi korumanız için önemli ve gereklidir.

Siber saldırganların, parolaları tahmin etmek veya “brute force (kaba kuvvet)” saldırıları yapmak için geliştirdiği karmaşık metodların zorluğuyla karşı karşıyayız, ve saldırganlar gün geçtikte sürekli olarak bu konuda daha iyi olmakta. Bu şu demektir; parolalarınız eğer güçsüzse veya kolay tahmin edilebilir durumdaysa saldırganlar tarafından ele geçirilebilir. Kendinizi bu durumdan korumanın önemli adımlarından birisi, güçlü parolaların kullanılmasıdır. Parolanız ne kadar fazla karakter içeriyorsa, parolanız o kadar güçlü ve zor tahmin edilebilir. Ancak, uzun ve karmaşık parolaları hatırlamak zor olabilir. Böyle bir durumda size, basit tümcecik veya kolay hatırlanan fakat zor ele geçirilen cümlelerden oluşan parolaları kullanmanızı öneriyoruz. İşte bir örnek;

Kral Julian nerede? (Sema: örneği ne ile değiştirelim ?)

Örnekteki parolayı güçlü yapan 19 karakter olmasının yanı sıra büyük harf ve özel karakter kullanılmış olmasıdır (boşluklar ve noktalama işaretleri de özel karakterdir). ‘a’ harfi yerine ‘@’, ‘o’ harfi yerine sıfır (0) rakamı kullanılması gibi harf yerine sayı veya özel karakter kullanımı, parolayı daha güçlü hale getirecektir. Ayrıca, eğer bir ağ sitesinde veya yazılımda parola karakter sayısı için bir sınırlandırma varsa, izin verilen maksimum parola karakter sayısını kullanınız.

Parola güvenliği

Parola kullanırken dikkatli olmalısınız. Art niyetli kişiler, kullandığınız parolayı kolayca ele geçirebilir veya kopyalayabilir durumdaysa parola kullanmanın bir yararı olmayacaktır

1. Her cihazınız veya hesabınız için farklı parolalar kullandığınızdan emin olun. Örneğin, işte veya banka hesabınızda kullandığınız parolayı Facebook, Youtube veya Twitter gibi özel hesaplarınızda kullanmayın. Böylece, eğer bir hesabınız ele geçirilirse diğer hesaplarınız güvende olacaktır. Hatırlamanız gereken çok fazla parola varsa -ki bu çok yaygındır-, parola yönetim programı kullanmayı düşünebilirsiniz. Parola yönetim

programı, bütün parolalarınızı güvenli bir şekilde saklayan özel bir programdır. Bu yolla hatırlamanız gereken parolalar sadece bilgisayarınızın ve parola yönetim programınızınki olacaktır.

2. Kullandığınız herhangi bir parolayı veya parola oluştururken kullandığınız stratejiyi iş arkadaşlarınız dahil kimseyle paylaşmayın. Parolanın kişiye özel olduğunu ve bu özel bilginin birisi tarafından bilinmesi durumunda daha fazla güvende olmayacağını unutmayın. Parola, eğer istemeyerek paylaşıldıysa veya ele geçirildiğine inanılıyorsa, hızlı bir şekilde değiştirilmelidir.
3. Kolay tahmin edilebilir ve sık kullanılan parola kullanmaktan kaçının. Örneğin, "Sakla samanı gelir zamanı" yaygın bilinen bir deyim olduğundan iyi bir parola değildir.
4. Otel, kütüphane gibi yerlerde bulunan genel kullanıma açık bilgisayarlarda iş veya banka hesabınızla ilgili herhangi bir işlem yapmayın. Çünkü bu bilgisayarlar herkes tarafından kullanabilir ve klavye hareketlerinizi kaydeden zararlı yazılımlar bulaşmış olabilir. İş veya banka hesaplarınızla ilgili işlemleri sadece güvenilir bilgisayar ve mobil cihazlar üzerinden yapın.
5. Kişisel sorulara cevap vermeniz gereken internet sitelerinde dikkatli olun. Bu sorular kullandığınız parolayı unuttuğunuzda ve sıfırlamak istediğinizde kullanılır. Problem, bu soruların cevaplarının internet üzerinde veya sizin Facebook sayfanızda bulunabilmesi durumundan kaynaklanmaktadır. Bu sorulara cevap verirken, cevapların genele açık ortamda kolayca bulunmadığından veya sizin oluşturduğunuz hayali bir bilgi olduğundan emin olun. Parola yönetim programları, bu bilgilerin saklanmasında da yardımcı olabilir.
6. Birçok çevrimiçi hesap iki adımlı doğrulama olarak da bilinen iki faktörlü doğrulama seçeneği sunar. Bu seçenek ile oturum açabilmeniz için parola kullanmanızın yanı sıra telefonunuza gönderilen kod gibi artı bir şeye daha ihtiyacınız vardır. İki faktörlü doğrulama seçeneği, yalnızca parola kullanımından daha güvenlidir. Mümkünse, her zaman bu seçenek kullanılmalıdır.
7. Mobil cihazlar, güvenlik için genelde PIN kullanır. PIN'in de bir parola olduğunu unutmayın. Kullandığınız PIN ne kadar uzunsa, o kadar güvenlidir. Ayrıca, birçok mobil cihaz, PIN yerine parola kullanımına izin vermektedir.

Son olarak, bir hesabı artık kullanmayacaksınız, kapattığınızdan, sildiğinizden veya pasif hale getirdiğinizden emin olun.

Not : Kurumun parola politikası eklenecek

B.4 - Temiz Masa Temiz Ekran

Kurumun temiz masa temiz ekran politikası ve varsa Modül B girişte yer alan bilgilerle oluşturulacak.

B.5 - Fiziksel Güvenlik

Kurumun fiziksel güvenlik süreçleri ve varsa Modül B girişte yer alan bilgilerle oluşturulacak.

B.6 - Erişim Kontrolleri

Kurumun erişim kontrolü süreçleri ve varsa Modül B girişte yer alan bilgilerle oluşturulacak.

B.7 - BYOD

Kurumun BYOD kuralları ve varsa Modül B girişte yer alan bilgilerle oluşturulacak.

B.8 - Güvenli İşletim Sistemi Kullanımı

B.8.1 – Konu anlatımı:

- İşletim sistemlerinin güvenlik açısından karşılaştırması
- Orijinal işletim sistemi kullanmak
- Crackli işletim sistemi kullanmak
- İşletim sistemi üzerindeki açıklıklar
- İşletim sistemi güncellemeleri
- İşletim sistemleri nasıl ele geçirilir?

B.9 - Bulut Bilişim

B.9.1 – Konu anlatımı:

“Bulut Bilişim” bireylerin ve organizasyonların hızlı bir şekilde geçiş yaptıkları güçlü bir teknoloji. “Bulut” farklı bireyler için farklı anlamlara geliyor olabilir ancak genel olarak sizin verilerinizin internet üzerinden yönetilmesi ve saklanması için bir hizmet sağlayıcının kullanılması anlamına gelir. Bulutun tek avantajı kolaylıkla ve farklı cihazlardan dünyanın herhangi bir yerinden verilerine erişmeniz ve senkronize etmeniz değildir, aynı zamanda dilediğiniz kişiyle dilediğiniz bilgilerinizi paylaşabilirsiniz. Bu hizmetleri “Bulut” olarak adlandırmamızın nedeni, verilerin fiziksel olarak nerede saklandığının genellikle bilinmemesidir.

Bulut bilişime verilebilecek örnekler; Google Docs kullanılarak dokümanların yaratılması, Dropbox kullanılarak dosya paylaşımı, Amazon Cloud üzerinde kendi sunucunuzu kurmak, Apple iCloud üzerinde müzik ya da resim dosyalarını barındırmak olabilir. Bu çevrimiçi hizmetler sizin daha üretken olmanızı sağladığı gibi, kendilerine özgü riskleri de beraberinde getirirler.

Bu hizmetleri kullandığınızda, kişisel verilerinizi yabancılara teslim ediyor ve onlardan bu verileri hem güvenli hem de erişilebilir tutmalarını bekliyorsunuz. Hal böyle olunca da seçiminizi akıllıca yaptığınızdan emin olmak istersiniz. İş bilgisayarlarınız ve iş ile ilgili bilgileriniz için, Bulut bilişim hizmetlerini kullanıp kullanamayacağınızı, yöneticinizle görüşmelisiniz. Eğer izniniz varsa, lütfen hangi Bulut bilişim hizmetlerini kullanabileceğinizi ve bunları nasıl kullanacağınızı anlatan politikaların hangileri olduğunu doğrulayın. Eğer kişisel olarak Bulut bilişim hizmeti kullanmayı düşünüyorsanız, aşağıdakileri göz önüne alın.

1. Destek: Yardım almanız ya da bir sorunuzun cevaplanması ne kadar kolay? Arayabileceğiniz bir telefon numarası ya da iletişime geçebileceğiniz bir e-posta adresi var mı? Destek için halka açık forumlar ya da internet sitelerinde Sıkça Sorulan Sorular sayfası gibi başka seçenekler var mı?

2. Basitlik: Bu hizmeti kullanmak ne kadar kolay? Daha karmaşık hizmet, sizin hata yapmanızı ve yanlışlıkla bilgilerinizi açığa çıkarmak ya da kaybetmenizi kolaylaştırır. Anlaması, yapılandırması ve kullanımı kolay bir Bulut hizmet sağlayıcısı seçin.

3. Güvenlik: Bilgisayarınızdan Bulut ortamına veriniz nasıl iletiliyor, bağlantı şifreleme yöntemleri ile güvenli mi? Verileriniz nasıl saklanıyor, şifrelenerek mi ve eğer evet ise, kimler verilerinizin şifrelerini çözebilir?

4.Hizmet Koşulları: Bir dakikanızı ayırın ve Hizmet Koşulları bölümünü okuyun (genellikle okunması oldukça kolaydır). Verilerinize kimlerin erişebileceğini ve kanuni haklarınızın neler olduğunu öğrenin.

Verinizi Güvenli Hale Getirmek

Bulut hizmetini seçtikten sonraki adım, bu hizmeti uygun şekilde kullanıyor olduğunuzdan emin olmaktır. Verinizi nasıl eriştiğiniz, verinizi nasıl paylaştığınız, dosyalarınızın güvenliği üzerinde, diğer her türlü şeyden daha büyük bir etkiye sahiptir. Uygulayabileceğiniz önemli adımlardan bazıları:

1. **Kimlik Doğrulama**: Bulut hesaplarınız için güçlü, benzersiz birer parola kullanın. Eğer hizmet sağlayıcınız iki aşamalı doğrulama (2FA) destekliyorsa, aktif hale getirmenizi kesinlikle tavsiye ediyoruz.
2. **Dosya / Dizin Paylaşımı**: Bulut, paylaşımı gayet basit hatta bazen fazla basit hale getirir. Olumsuz bir senaryoda, siz yanlışlıkla dosyalarınızı hatta tüm dizinlerinizi, internet üzerinden halka açık hale getirebilirsiniz. Kendinizi korumak için en iyi yöntem, varsayılan olarak hiçbir dosya/dizin paylaşmayıp, ihtiyaç oldukça belirli kişi ya da grouplara yetkilendirme yapabilirsiniz. Erişim ihtiyacı ortadan kalktığında, yetkilerini kaldırın. Bulut hizmet sağlayıcınız dosya ve dizinlerinize kimlerin erişim izni olduğunu kolayca izleyebileceğiniz bir yöntem sağlıyor olmalıdır.
3. **Bağlantılar kullanarak dosya ve dizin paylaşımı**: Bulut hizmetlerinin ortak bir özelliği de dosya/dizinlerinizi gösteren bir web bağlantısı oluşturmalarıdır. Bu özellik, basitçe bu bağlantıyı paylaşarak herhangi biriyle bu dosyaları paylaşmanızı sağlar. Az da olsa güvenli görünen bu yaklaşım ile, bağlantıyı bilen herkesin kişisel dosya ya da dizinlerinize erişebilir. Siz bağlantıyı tek bir kişiye gönderseniz de, o kişi bu bağlantıyı başka birine gönderebilir, o da başkaları ile paylaşabilir ya da arama motorlarında görünebilir. Eğer bu şekilde paylaşım yapıyorsanız, ihtiyaç kalmadığında bağlantıları pasif hale getirin, ya da eğer mümkünse, bağlantıyı bir parola ile koruyun.
4. **Ayarlar**: Bulut hizmet sağlayıcınız tarafından sunulan güvenlik ayarlarını inceleyin. Örneğin, eğer bir başkası ile bir dizin paylaşıyorsanız, sizin bilginiz dışında onlar da başkaları ile verilerinizi paylaşabiliyorlar mı?
5. **Antivirüs**: Bilgisayarınızdaki ya da verilerinizi paylaştığınız herhangi bir bilgisayardaki antivirus uygulamasının en güncel sürümünün kurulu olduğundan emin olun.

Paylaştığınız bir dosyaya virus bulaştığında, aynı dosyaya eriştiğiniz diğer bilgisayarlara da bulaşacaktır.

6. **Yedekleme**: Bulut hizmet sağlayıcınız verilerinizi yedekliyor olsa bile, kendiniz düzenli olarak yedeklerinizi alma seçeneğini değerlendirin. Bu, sadece hizmet sağlayıcınızın iflası, kapanması ya da herhangi bir sebeple erişilemez olması durumunda verilerinizi korumakla kalmaz, aynı zamanda büyük miktardaki verilerde Bulut üzerinden yedekten dönmeye kıyasla çok daha kolay bir geri dönüş sağlar. Bir de, Bulut hizmet sağlayıcınızın dosyalarınızı ne kadar sıklıkla yedeklediğini, dosyalarınızın önceki sürümlerine geri dönme imkanı verip vermediklerini ve yedeklerinizi ne kadar sure ile erişilebilir tuttuklarını kontrol edin.

B.10 - Sorumluluklarınız

B.10.1- Konu anlatımı:

Bu bölümde, kurum çalışanlarından beklentiler anlatılacak, kuruma özel “bilgi güvenliği olaylarını bildirim e-posta adresi, telefonu”, “kurumun bilgi güvenliği yöneticisi”, kurum çalışanlarının bireysel sorumlulukları (politikaları okumak, uygulamak, vb.) anlatılacak.

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.