Haberleşme ve İletişim Güvenliği

Elk. Müh. Alpaslan Güzeliş
alpaslan.güzelis@emo.org.tr

Elektronik haberleşme ve iletişim; her türlü işaret, sembol, ses, görüntü ile verinin, yani bilginin elektronik araçlarla gönderilip alınması ve iletilmesidir. Bunun için kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve benzer çeşitlilikte iletim sistemleri kullanılmaktadır. Son yıllarda elektronik ile bilgisayar sistemlerinin hızla gelişmesi haberleşme ve uzak iletişimde de sayısız olanak sağlamıştır. Günümüzde ülkelerin, uluslararası kurumların, kuruluşların ve elektronik haberleşme sektörünün önemli ilgi alanlarından birini de güvenlik oluşturmaktadır. Güvenli bir altyapıda; veri bütünlüğü, özel yaşam ve gizlilik korunur, yetkisiz erişimler engellenir, sistemin devamlılığı sağlanır.

Bilgi ve iletişim teknolojilerinin (BİT) sonucu ortaya çıkan yeni kullanım alanları, güvenlik konusunda alınan önlemlerin sürekli gözden geçirilmesini gerektirmektedir. Konu üzerinde gerek ulusal, gerekse uluslararası kurum ve kuruluşlar arasında sürdürebilir bir eşgüdüm de önemlidir. Gecikmeksizin çözümler üretilmelidir.

Haberleşme ve İletişim Altyapısında Güvenlik Tehditleri ile Zayıflıklar;

Güvenlik tehditleri:

Yetkisiz olarak ve yetki aşımıyla güvenlik duyarlıklı alanlara girilmesi,

Yetkisiz olarak veya yetki aşımıyla silme, ekleme, değiştirme, geciktirme yapılması. Ayrıca başka bir ortama kaydedip yayma yoluyla veri gizliliğinin, bütünlüğünün ve devamlılığının bozulması,

Donanım-yazılım bileşenlerinin, ulusal düzenleme ile ulusal ve uluslararası standartlarca belirlenen gereklilikleri yerine getirmesinin, kısmen veya tamamen engellenmesi,

Deprem, sel, su baskını, yangın gibi doğal afetler ile grev ve lokavt durumu,

Kullanıcıyı yanıltarak doğru tarafla elektronik haberleşmede bulunduğu izleniminin verilmesi,

Elektronik haberleşmenin yasal olmayan bir şekilde izlenmesi ve dinlenmesi,

Doğru olmayan bir bilginin üretilerek bu bilginin başka bir taraftan alındığının iddia edilmesi veya başka bir tarafa gönderilmesi,

Elektronik haberleşme altyapısının kısmen veya tamamen hizmet veremez duruma getirilmesi. Altyapıya ait kaynakların, hizmet sunumunu aksatacak şekilde tüketilmesi.

Zayıflıklar:

Gelecekte gerçekleşmesi olası tehditlerin öngörülememesi,

Bir sistemin ya da iletişim protokollerinin tasarımında yapılan yanlışlıklar,

Bir sistemin ya da protokolün oluşturulması sırasında ortaya çıkan sorunlar,

Geliştiricilerin hataları,

Uygulayıcıların hataları,

Sistemin iç iletişimi sırasında oluşan uygunsuzluklar ve yetersizlikler.

Güvenlik Konusunda Kurum, Kuruluş ve Kullanıcıların Yerine Getirmesi Gereken Sorumluluklar;

1) Kurum ve kuruluşların yerine getirmesi gereken sorumluluklar:

Yasalar, haberleşme ve iletişim güvenliği konusunda düzenleyici kurumlar ve işleticilere sorumluluklar yüklemektedir.

Düzenleyici kurumlar, yasalar doğrultusunda oluşturdukları yönetmelik ile tebliğlerle haberleşme ve iletişim için güvenlikli altyapıların oluşmasını sağlamakla yükümlüdür.

Ülkemizde 2008 yılında kabul edilen 5809 Sayılı Elektronik Haberleşme Yasasıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, elektronik haberleşmenin olağanüstü durumlar nedeniyle sekteye uğramaması için gerekli önlemleri almakla yükümlü kılınmıştır. Buna ek olarak da BTK'nın (Bilgi Teknolojileri ve İletişim Kurumu);

Kişisel veri ve gizliliğin korunması,

Olağanüstü durumlarda haberleşmenin kesintisiz sürmesi için gerekli önlemlerin alınması,

Erişim yükümlülükleri,

Elektronik haberleşme ağlarının bütünlüğünün devam ettirilmesi,

İzinsiz erişime karşı ağ güvenliğinin sağlanması gibi konularda yetkili olduğu ve yükümlülük getireceği vurgulanmıştır.

BTK'nın yapmış olduğu çalışmalar sonucunda hazırlanan Elektronik Haberleşme Güvenliği Yönetmeliği, 2008 yılında yürürlüğe girmiştir. Bu yönetmelikte elektronik haberleşmede güvenliğin usul ve esasları ile işletmecilerin yükümlülükleri tanımlanmıştır. İşletmecilerinden fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenirliliği ile personel güvenirliğinin sağlanması

istenmektedir. Ayrıca, Tehditlerden ve yetersizliklerden kaynaklanan risklerin, olabildiğince yok edilerek azaltılmasına ilişkin alacakları önlemler de bu yönetmelik kapsamındadır.

Haberleşme ve iletişim güvenliğinde işletmelerce (servis sağlayıcılarca) göz önünde tutulması gereken ilkeler:

Nesnel şartlar aksi bir durumu zorunlu kılmadıkça niteliksel ve niceliksel devamlılık, ayrım gözetmeme, düzenlilik, saydamlık ve kaynakların etkin kullanılması,

Tüketici haklarının korunması,

Sürdürülebilir hizmet kalitesi ve bunun yükseltilmesi,

Ulusal ve uluslararası düzenleme ile standartlara uygunluk.

Tesis binaları içinde fiziksel alan güvenliği:

Giriş ve erişim yetkisi ile bu yetkinin kapsamı işletmeci tarafından önceden tanımlanıp giriş ve erişim yetkili kişilerle sınırlandırılmalıdır,

Ziyaretçi giriş ve çıkışlarında gerekli kontroller yapılarak tarih, saat, kimlik gibi bilgiler kaydedilmelidir. Her ziyaretçinin sadece izin verilen yerlere giriş ve çıkışı sağlanmalıdır,

Tüm personel ve personel harici kişiler, kimlik bilgilerini, yetki ve erişim seviyelerini açık bir şekilde görünür kılacak giriş veya kimlik kartı taşımalıdır,

Güvenlik duyarlıklı alanlara giriş ve erişim yetkisi, düzenli olarak gözden geçirilerek güncellenmeli ve gereğinde iptal edilmelidir.

Bina dışı alanlardaki tesislerde güvenlik önlemleri:

Sahada yer alan haberleşme altyapısına ait insansız bina, kule, dolap ve kutu gibi güvenlik riski oluşturabilecek altyapı bileşenlerine erişim kontrol altında tutulmalıdır. Yetkisiz kişilerin kolaylıkla ulaşamayacağı şekilde tesis edilmelidir,

Güvenlik gereken fiziksel alanlarda ek olarak alınması gereken önlemler:

Kötü amaçlı müdahaleleri engellemek için planlanmamış çalışmalardan kaçınılmalıdır,

Ses ve video kayıt cihazlarının, güvenliğe duyarlı alanlara izinsiz olarak girişini engellemek için gerekli önlemler alınmalıdır,

Haberleşme tesislerinin dış tehditlere karşı korunması amacıyla fiziksel önlemler de planlanıp uygulanmalıdır.

Personel güvenirliliği:

Haberleşme ve iletişim altyapısında çalıştırılacak teknik personel, konusunda yeterli meslek deneyimine sahip ya da eğitim almış olmalıdır. Bu personelin görev tanım ve sorumluluklar açıkça belirtilmelidir,

Altyapıda çalıştırılacak personelden adli sicil kaydı istemelidir,

Personelin haberleşme gizliliğine, ulusal güvenliğe ve kamu düzenine aykırı davranışta bulunmaması için her türlü önlem alınarak, işlerin ve hizmetlerin düzenli yapılması sağlanmalıdır.

Veri güvenliği:

Veri erişim yetkisi ve bu yetkinin kapsamı önceden belirlenip kayıt altına alınmalıdır,

Veriye erişimde, yetki sınırlamasına olanak sağlayan teknolojilerin kullanılması konusunda gerekli olan yatırımlar eksiksiz yapılmalıdır.

Donanım-yazılım güvenliği ve güvenirliliği:

Donanım-yazılımın ulusal düzenleme ile ulusal ve uluslararası standartlara uygunluğu sağlanmalıdır,

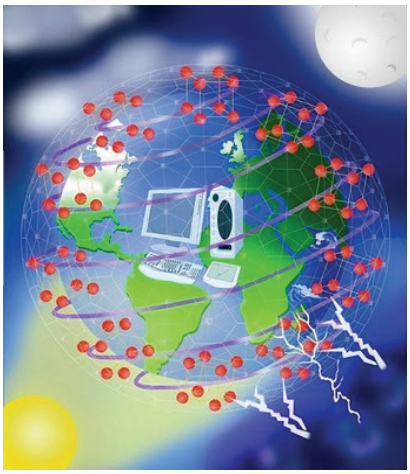
Aynı fiziksel alanda ya da farklı fiziksel alanlarda bulunan donanım-yazılım bileşenleri arasındaki iç haberleşmeyi sağlayan kablolu-kablosuz ağ yönetimi, sadece yetkili kişiler tarafından erişilecek şekilde şifrelenmelidir,

Donanım-yazılım bileşenlerinin, yasal olmayan dinleme ve izleme tehdidi oluşturacak unsurları içerip içermediği belirlenmelidir. Bunun için satın alma, kullanım, bakım ve onarım sırasında düzenli kontrolleri yapılmalıdır. Bu tür bir unsurun saptanması durumunda ilgili bileşenin kullanımına son verilmelidir. Bu durum kayıt altına alınıp raporlandıktan sonra oluşan tehdidi yok edecek önlemler ivedilikle alınmalıdır,

İşletmeci, haberleşmenin gizliliği, bütünlüğü ve devamlılığı için kritik donanım-yazılım bileşenlerini belirleyerek bunların yedekli çalışması konusunda da önlemler almalıdır.

2008 yılında yayınlanan Elektronik Haberleşme Güvenliği Yönetmeliği'ne göre işletmecilerin (servis sağlayıcıların) yükümlüğü:

Söz konusu standart, Merkezi güvenlik sistemlerinde bilgi güvenliği sisteminin yönetimi için geliştirilmiştir. İşletmeci, TS ISO/IEC 27001 veya ISO/IEC 27001 standardına uygunluğu sağlamakla yükümlüdür.



İşletmeci, yetki alımından sonra bir yıl içinde bu standarda uygunluğu sağlamak zorundadır.

İşletmeci, tehdit ve zayıflıklarla ilgili olmak üzere risk analizini yılda en az bir kere kendi bünyesinde veya tarafsız kuruluşlarca yaptırılmasını sağlamalıdır. İşletmeler alt yüklenici firmalardan doğan güvenlik sorunlarından da sorumludur.

2) Kullanıcılar tarafından alınması gereken güvenlik önlemleri:

Sabit telefonlarda **güvenlik önlemleri:**

Sabit telefonlarda devamlılığın sağlanması ile yetkisiz kişilerce yasadışı olarak dinleme, izleme ve kullanımını engellemek için kullanıcıların da alması gereken bazı önlemler vardır.

İşletmecinin sorumluluğunda bulunmayan bina içi sabit telefon hatlarının sıva altı ve dışarıdan paralel bağlantı yapılmayacak şekilde olmalıdır,

Kordonsuz telefon kullanımında, enerji kesintilerinde haberleşme devamlılığını sağlamak için, kesintiden etkilenmeyen ayrı bir telefonun da paralel bağlı olarak hazır bulundurulması,

Gezgin telefonlarda; güvenlik önlemleri:

IMEI (International Mobile Equipment Identity) numarası mutlaka telefon dışında da kolay ulaşabilecek bir yere kaydedilmelidir. Bu, telefonların kaybolması veya çalınması durumunda bulunmasını kolaylaştırır. IMEI numarası telefonlarda *#06# tuşlanarak tespit edilebilir.

Kamuya açık ve güvenirliği olmayan alanlarda kablosuz internet bağlantısı yapmaktan kaçınılmalıdır,

Telefona uzaktan erişimi olanaklı kılan ve içeriği silebilecek uygulamalar tercih edilmelidir,

Kullanıcı bilgisi dışında telefona erişimi engellemek için gelen uygulama taleplerinde dikkatli davranılmalıdır. Güvensiz, şüpheli ve gereğinden fazla yetki isteği olan uygulamalara izin verilmemelidir,

Telefon içindeki veriler sıkça yedeklenmelidir.

Şifre güvenliği:

Özelikle bilgisayarda ve internete erişimde şifrelerin güçlü olarak değerlendirilen yapıda olmasına özen gösterilmelidir. Şifreler, kolay tahmin edilebilir ardışık sayı dizilerinden oluşmamalıdır. Ad, soyadı, doğum ve evlilik tarihi gibi sayı ve harfleri kullanmaktan kaçınılmalıdır. Giriş yapılan site ve sitemlerin her birinde farklı olmak üzere, karşı sistemin verdiği olanaklar doğrultusunda en fazla karakterin yer alabileceği şifreler tercih edilmelidir. (Sekiz karakter güçlü olarak değerlendirilmektedir.) Şifrelerin rakam ve harflerden karmaşık bir düzen içinde oluşması sağlanmalıdır.

Zararlı yazılımlara karşı korunma:

Zararlı yazılımlara karşı korunma, kullanıcıların kişisel bilgilerinin ele geçirilmemesi, maddi kayıplara uğramaması ve cihazlarının zarar görmemesi için uygulanması gereken bir zorunluluktur. Ücretli veya ücretsiz anti-virüs programlarının sürekli güncellenerek sistemlerde yüklü olması gerekmektedir. Tam bir güvenlik sağlamasalar da kişisel ve kurumsal zararların en az seviyelere inmesine katkısı olmaktadır.

Bilgi-İletişim Teknolojileri ve Karayolu Güvenliği

Son yıllarda bilgi ve iletişim teknolojilerinin getirdiği olanaklar, taşıt radarları, navigasyon, elektronik yol ve hava durumu bildirimi bunlardan bir kaçıdır. Sürücünün, yolculuk sırasında kural ihlali yaparak haberleşme ve iletişim cihazlarını kullanması, dikkat dağıtıcı bir etmen olarak kaza olasılıklarını ortaya çıkarmaktadır.

17 Mayıs Dünya Telekomünikasyon ve Bilgi Toplumu Günü'nün 2013 yılı teması, 'BİT ve Karayolu Güvenliği Geliştirme' olarak belirlenmiştir. Birlik, yolculuklar anında hatalı kullanıma dikkat çekmeye çalışmaktadır. Kara taşıtları için geliştirdiği standartların yaygınlaşması konusunda çaba göstermektedir. Bu standartların sonucu geliştirilen eller-serbest (Hands-Free) kullanım benzeri kitler, riskin düşmesine büyük ölçüde olanak yaratmaktadır.

Dünyada en çok trafik kazasının oluştuğu ülkelerden biri olan Türkiye'de de, sürüş anında BİT'nin güvenli kullanımıyla ilgili bilincin oluşmasına gereksinim vardır. Ayrıca, Özellikle kent içlerinde kural ihlallerinin azaltılmasına ve düzenliği trafiği sağlamaya dönük; trafik yönetim ve plaka tanıma sistemleri, sürdürülebilir sinyalizasyon gibi BİT'in yeni olanakları olabildiğince yaygınlaştırılmalıdır.

KAYNAKÇA

5.11.2008 kabul tarihli 5809 Sayılı **'Elektronik Haberleşme Kanunu.'**

20.7.2008 Resmi Gazete tarihli **'Elektronik Haberleşme Güvenliği Yönetmeliği.'**

23.3.2011 Resmi Gazete tarihli **'Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulamasına İlişkin Tebliğ.'**