Dijital sağlık uygulamalarında siber güvenlik

Doç. Dr. Bilgin Metin

İstanbul Teknik Üniversitesi Elektronik Haberleşme Mühendisliği Bölümünden mezun oldu. Boğaziçi Üniversitesinde Elektrik-Elektronik Mühendisliği alanında yüksek lisans ve doktorasını tamamladı. Özel sektörde ağ sistemleri ve ağ güvenliği tasarımı, desteği ve kurulumu konularında danışmanlık hizmeti verdi. 2007 yılında Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Bölümünde yardımcı doçent olarak çalışmaya başladı. 2014 yılında doçent unvanını aldığı aynı yerde görevine devam etmekte, ayrıca 2017 yılından beri Boğaziçi Üniversitesi YBS Siber Güvenlik Merkezinin Yöneticiliğini yapmaktadır.

Sağlık kuruluşları; savaş, terörizm, salgın ve doğal afetler gibi olağanüstü durumlarda hayati öneme sahip oldukları için kritik bir altyapı olarak ele alınmalıdır. Özellikle pandemi sebebiyle evlerde karantinada kaldığımız şu günlerde teletıp uygulamalarının önemi daha fazla anlaşıldı ve bu kritik altyapıların önemli bir parçası haline geldiler. COVID-19 döneminde yaşananlar mevcut sağlık hizmetlerinin sürdürülebilir olmadığını bir kere daha gösterdi. Halbuki teletıp sayesinde hastanelere uzak bölgelerde yaşayan insanlar da sağlığa daha kolay erişebilirler. Vatandaşların hastanelere gitmeye çekindiği, şu anda yaşadığımız gibi pandemi ortamlarında insanlar birtakım sağlık hizmetlerini evlerinden alabilirler. Teletıp teknolojilerinin bu beklentileri en iyi şekilde karşılayabilmesi için siber saldırılar karşısında da güvenle hizmet verebilmesi gerekiyor (1-10).

Sağlık Altyapılarında Dijitalleşmenin Getirdiği Riskler

Dijitalleşmenin olanca hızıyla ilerlediği günümüzde sağlık sistemleri de bu dönüşümde ilk sıralarda yer alıyor. Sağlık kuruluşlarındaki dijitalleşmenin en önemli sorunlarını bilgi güvenliği açısından dört kısımda ele almak mümkündür:

1) Hastane altyapılarındaki entegrasyon sorunları: Eski sistemlerle yeni sistemlerin bir arada kullanılmasından kaynaklanan zorluklar, sayısı her geçen gün artan siber saldırılar ve nesnelerin internetiyle hayatımıza hızlıca giren cihaz ve uygulamalar... Sağlık kurumlarındaki bilgi sistemleri insan hayatıyla ilgili olduğu için en yüksek kalite standartlarını sağlayacak şekilde üretilir. Bu yüzden, eski sistemleri tamamen kaldırıp yenisini satın almak çok maliyetli olduğu için eski ve yeni sistemler genellikle beraber kullanılır. Farklı üreticilere ait cihaz ve yazılımların bir arada kullanılması da siber tehditlerin izlenebilirliğini zorlaştırmakta ve güvenlik zafiyeti oluşturmaktadır. Güvenlik zafiyetleri çıktığında uygun yamaların zamanında yüklenmesi çok önemlidir. Destek süresi dolduğu için artık güvenlik yaması yayınlanmayan eski sistemlerin diğerlerinden yalıtılmış kontrollü bir ağ içinde kullanılması gerekir.

2) Nesnelerin interneti ve mobil uygulama ve cihazlar: İkinci konu ise nesnelerin interneti kavramının gelişmesiyle hayatımıza daha fazla giren sağlık cihazları ve teletıp uygulamalarıdır. Bu sistemlerin çoğu, mobil uygulamalar şeklinde akıllı telefonlar üzerinde çalışmaktadır. Bu cihazlar hem adet hem çeşitlilik açısından çok fazla oldukları ve yoğun miktarda kişisel bilgi barındıkları için siber saldırıların hedefi haline geldiklerinden aktif bir şekilde bilgi güvenliklerinin sağlanması gerekmektedir. Mobil uygulamaların dijital sağlık teknolojilerinde kullanımı artmaktadır. Mobil uygulamalar, bulut sistemleri de dahil teletıp uygulamaları ile direkt bağlantılı oldukları için kritik zafiyetlerin kaynağı olabilir.

3) İnsan faktörü: Kullanıcılarda ve üst yönetimde bilgi güvenliği farkındalığı eksikliği, sosyal mühendislik saldırıları ve sistem arızalarına neden olacak ihmallere yol açmaktadır.

4) Bilgi güvenliği yönetişimi eksikliği: Bilgi güvenliği yönetişimi iç ve dış paydaşların etkin koordinasyonunun sağlanması, risk değerlendirme çalışmalarının yapılması, yasalar, standartlar ve en iyi uygulamalarla uyumluluk olarak açıklanabilir. Bu konuda aşağıdaki başlıklara dikkat edilmelidir:

a) Hastaneler çok paydaşlı yapılardır. Bazı durumlarda röntgen, tomografi, MR gibi sağlık sistemleri hastane içinde anlaşmalı kurumlarla beraber işletilmektedir. Bu durumda, yönetimi başka kuruluşta olan bilgisayarlar hastane ağı içinde kullanılmaktadır veya bu firmalar VPN üzerinden hastane sistemine kontrolsüz erişim sağlayabilmektedirler. Bir sağlık kuruluşu kendi sistemlerindeki güvenlik açıklarını en iyi şekilde kapatsa bile sistemlerin farklı kuruluşlarca beraber kullanılması bilgi varlıkları üzerinde yetki kargaşasına sebep olabildiği için gerekli önlemler alınamamaktadır. Bu konunun çözümü, etkin bilgi güvenliği yönetişimi ile mümkündür.

b) Sağlık kuruluşlarının stratejileri içinde siber güvenliğe yer verilmeli ve üst yönetimin liderliğinde kurumsal işletme risklerden birisi olarak ele alınmalıdır. Etkin risk değerlendirmesi yapılabilmesi için teletıp sistemleri başta olmak üzere altyapıdaki bilgi varlıklarının eksiksiz bir envanteri hazırlanmalıdır. Üzerlerindeki güvenlik zafiyetleri ve siber güvenlik tehditleri ortaya konarak ilgili riskler tanımlanmalıdır. Bu riskleri azaltmak için mevcut kontrollerin açıklamaları ve bu kontrollerin yeterince test edildiğini gösteren kanıtlar kayıt altına alınarak riskler azaltılmalıdır. Risk yönetimi için nicel ya da nitel bir yaklaşım sergilenebilir. Önemli olan, risk değerlendirmesinin periyodik olarak ele alınan bir süreç olarak görülmesi, taşınma ve altya-

pıdaki değişiklikler söz konusu olduğunda yeniden ele alınmasıdır.

c) Standartlara ve en iyi uygulamalara uyumluluk, içerdikleri kontrol noktaları ile etkin bir denetim imkânı sunar. Genel manada ISO/TR 27001 Bilgi Güvenliği Yönetimi Standardının (11) uygulanması artık yaygın kabul görmüştür. Bunun yanında teletıp açısından ISO 14971:2019 Medikal Cihazlara Risk Yönetimi Uygulaması Standardının (12) uygulanması önemli olacaktır. Riskleri her yönüyle ele almak gerekir. Tıbbi cihazların gün geçtikçe internete daha fazla "bağlanması" nedeniyle, yeni güvenlik risklerinin değerlendirilmesi ve belgelenmesi gerekmektedir. Çoğu üretici için bu sorun yeni bir durum değildir ancak ISO/TR 24971:2020 (13) Ek F, tıbbi cihaz şirketlerinin, cihazın kötüye kullanımıyla hiçbir ilgisi olmayan kullanıcılara veya hastalara yönelik çok gerçek riskleri ele alma ihtiyacını kabul eder ve güçlendirir. ISO/TR 24971:2020 Ek F dört sayfadan fazladır ve ISO 14971 ile siber güvenlik süreci ilişkisinin yanı sıra siber güvenlik ve veri güvenliği için risk yönetimini kapsar. Bu saydığımız hususlara dikkat edilmediğinde yaşanacak sıkıntılara örnek olması sebebiyle dünyadaki siber güvenlik olaylarına bir göz atalım.

Sağlık Kurumlarında Yaşanan Siber Güvenlik Olayları

Son yıllarda siber saldırı denilince akla hemen "zararlı yazılımlar" gelmektedir. Sağlık sistemlerinde kullanılan güncel olmayan sistemlerin oluşturdukları zafiyet konusunun en iyi örneği, 2017 yılında tüm dünyayı etkisi altına alan *WannaCry* adlı bilgisayar solucanıdır. Sağlık alanında çok hızlı dijitalleşen İngiltere'de bahsettiğimiz eski, yeni ve farklı sistemleri bir arada kullanma zorlukları yüzünden, *Wannacry* ağdaki tüm zafiyetli bilgisayarlara bulaşmıştı. Bilgisayarların büyük çoğunluğu şifrelenince acil servisler başta olmak üzere kayıtlar yapılamıyor, sosyal güvenlik ya da sağlık sigortaları kontrol edilemiyordu. Diğer taraftan yatan hastaların bağlı olduğu bilgisayarlar da kullanılamaz hale geldiğinden kaliteli sağlık hizmeti verilemiyor, yapılan kan testleri, tomografi, MR röntgen vb. test sonuçlarına erişilemiyordu (1). Etkilenen bilgisayarların bir kısmında artık Microsoft tarafından destek süresi bitmiş olan Windows XP işletim sistemleri kullanırken çoğunluğunda destek süresi devam eden ama güncellemeleri yapılamamış Windows 7 işletim sistemi yüklüydü. *WannaCry* sebebiyle 19 bin muayene randevusu iptal oldu. Tüm bu olayların maliyeti ise 92 milyon pound olarak ölçüldü (2).

Siber saldırı denince zararlı yazılımların oluşturduğu tehlikeler yanında "hizmet kesintisi saldırıları" (DoS) da örnek verilebilir. 2014 yılında Boston Çocuk Hastanesi, DDoS saldırısına maruz kaldı ve aynı ağda bulunan diğer hastaneler de internet bağlantılarını kaybettiler ve neredeyse bir hafta boyunca online sistemlerini kullanmakta problem yaşadılar. Bu saldırının hastaneye 300 bin dolardan fazla maddi zarar verdiği kayıtlara geçti (3). Kişileri telefon dolandırıcılığı gibi yöntemlerle kandırarak sistem parolası elde etme, sisteme giriş hakkını elde etme gibi yöntemler anlamında kullanılan "sosyal mühendislik saldırıları", siber güvenlik farkındalığı konusuyla bağlantılıdır. Örneğin 2015'te, siber korsanlar çalıntı bilgilerle yerel bir tıp merkezine 500 bin dolar değerinde reçeteli ilaç siparişi vermeye teşebbüs edince eczane çalışanlarının protokolleri doğru yerine getirerek, hastaneye doğrulama telefonu açması sayesinde saldırı engellenmişti (4). Ayrıca "oltalama saldırıları" dediğimiz kandırıcı nitelikli e-posta mesajları göndererek sistemlere zararlı yazılım yüklemeye teşebbüs etme yöntemi de sosyal mühendislik saldırıları olarak kullanılıyor (5).

ABD'nin Illinois eyaletinde 210 bin kişiye hizmet veren bir sağlık kurumu ise NetWalker adındaki bir zararlı yazılımın kurbanı oldu (6). Çekya'nın ikinci büyük hastanesi olan Bruno Şehir Hastanesi 14 Mart 2020'de uğradıkları siber saldırı sonucu hasta verilerini elle doldurmak zorunda kaldı. (7). Almanya'da ise 9 Eylül 2020'de yaşanan bir fidye yazılımı saldırısı sonucunda hastane sistemleri devre dışı kaldı, hastalar yakındaki bir hastaneye transfer edilirken bir hasta yaşamını yitirdi. (8) "Veri sızdırılması" da yine yoğun karşılaşılan bir siber saldırı türüdür. Sağlıkla ilgili kişisel veriler, hem dünyadaki ilgili yasalarla hem de ülkemizdeki 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında (9), özel nitelikli kişisel veri olarak tanımlanır ve şifreleme başta olmak üzere özel önlemlerle saklanmaları gerekir. ABD'de sağlık sistemleri de dahil olmak üzere kuruluşlar için bağışçı bilgilerini saklayan bir şirketin uğradığı siber saldırıda 46'dan fazla hastaneye ait bir milyondan fazla kişisel veri sızdırıldı (10).

Sonuç

Sağlık kurumları hem yoğun olarak kişisel veri içerdiği hem de bu çalışmada yer verdiğimiz sebeplerle savunması zayıf olduğu için siber korsanlar için cazip birer hedef haline gelmiştir. Siber güvenlik ihlalleri, hasta bilgilerinin çalınması ve hastanelere yapılan zararlı yazılım saldırılarını, dağıtılmış hizmet kesintisi (DDoS) ve sosyal mühendislik saldırılarını içerebilir. Hastanelerin altyapısından başlayıp hasta vücutlarındaki kalp pili gibi implante tıbbi cihazlara kadar geniş bir atak yüzeyine sahiptir. Siber saldırılar teletıp sistemlerine yönelik hasta güvenini azaltabilir, bu sistemleri çalışamaz hale getirerek insan yaşamını tehdit edebilir. Sağlık endüstrisinde bilgi güvenliği yönetişimi daha en başta dijital dönüşümün en önemli bileşenlerinden biri olarak ele alınırsa, işletme hedeflerine ulaşmada hem en ekonomik hem en verimli hem de bilişim risklerinin göz önünde tutulduğu altyapılar kurulabilecektir.

Kaynaklar

1) https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf (Erişim Tarihi: 03.05.2021).

2) https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ (Erişim Tarihi: 03.05.2021).

3) https://www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/ (Erişim Tarihi: 03.05.2021).

4) https://www.cisecurity.org/blog/business-email-compromise-in-the-healthcare-sector/ (Erişim Tarihi: 03.05.2021).

5) https://www.forbes.com/sites/daveywinder/2020/04/08/cyber-attacks-against-hospitals-fighting-covid-19-confirmed-interpol-issues-purple-alert/#1dd2dcd358bc (Erişim Tarihi: 03.05.2021).

6) Centers for Disease Control. (2020). "Using Telehealth Services." June 10, 2020. https://www.cdc.gov/ coronavirus/2019-ncov/hcp/telehealth.html (Erişim Tarihi: 03.05.2021).

7) https://www.scmagazineuk.com/coronavirus-test-results-delayed-cyber-attack-czech-hospital/article/1677194 (Erişim Tarihi: 03.05.2021).

8) https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/ (Erişim Tarihi: 03.05.2021).

9) Kişisel Verilerin Korunması Kanunu, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (Erişim Tarihi: 03.05.2021).

10) https://www.beckershospitalreview.com/cybersecurity/the-5-most-significant-cyberattacks-in-healthcare-for-2020.html (Erişim Tarihi: 03.05.2021).

11) ISO/IEC 27001 Information Security Management, https://www.iso.org/isoiec-27001-information-security.html, (Erişim Tarihi: 03.05.2021).

12) ISO 14971:2019 Medical Devices - Application of Risk Management to Medical Devices, https://www.iso.org/standard/72704.html (Erişim Tarihi: 03.05.2021).

13) ISO/TR 24971:2020, Medical Devices - Guidance on the Application of ISO 14971 https://www.iso.org/standard/74437.html (Erişim Tarihi: 03.05.2021).