EURASIAN RESEARCH INSTITUTE
e-bulletin
Analysis
04.02.2025 № 376

KAZAKİSTAN'DA DİJİTAL GÜVENLİK VE TEHDİTLER

Dijital dolandırıcılık, on yıllardır süregelen bir sorun olup geçmişi 1970'lerin başlarına, e-posta saldırılarının ortaya çıkışına kadar uzanmaktadır. O dönem bu tür dolandırıcılık için özel bir terim henüz kullanılmıyordu ve bu yöntem 1990'ların ortalarına kadar yaygınlaşmadı. O zamandan bu yana, çevrimiçi dünyada dolandırıcılar sahte e-posta adresleriyle büyük veri ihlallerinden elde edilen bilgilerin kötüye kullanılmasına kadar her şeyi denedi [Strandell, 2024]. Ancak, saldırıya uğrayan tek dijital kanal e-postalar olmadı. İlk cep telefon dolandırıcılıkları, çalkantılı 1980'lerde ortaya çıktı ve 1990'larda hızla yaygınlaştı. Örneğin, telefon sahipleri, bir aile üyesinin hesabına "hızlı bir şekilde" para göndermelerini isteyen mesajlar alıyordu. Şifre hırsızlığı, web sitesi saldırıları ve casus yazılımlar gibi diğer tehditler de bu süre zarfında dünya çapında endişe verici bir hızla yayıldı.

Bugün karşılaştığımız en büyük zorluklardan biri, çevrimiçi dolandırıcılığın çok daha kolay gerçekleştirilebiliyor olmasıdır. Hackerlar, teknolojideki gelişmelere ayak uydurarak yeteneklerini sürekli geliştirmektedir. Microsoft tarafından yapılan yakın tarihli bir anket, dünya genelindeki internet kullanıcılarının en çok sahtecilik, dolandırıcılık ve kötüye kullanım konusunda endişeli olduğunu göstermektedir. Microsoft'un Temmuz ve Ağustos 2023'te 17 ülkede gerçekleştirdiği ankette, katılımcıların %71'i yapay zeka destekli dolandırıcılıktan "çok" veya "biraz" endişe duyduğunu belirtti. Bu dolandırıcılıkların en yaygın şekli, ünlü bir kişiyi, bir devlet yetkilisini veya katılımcının tanıdığı birini taklit etmektir. Derin sahtekarlıklar (deepfake) ve cinsel ya da çevrimiçi istismar %69 ile ikinci sırada yer almaktadır. ChatGPT gibi sohbet botlarının anlamsız yanıtlar verdiği durumlar olarak tanımlanan yapay zeka halüsinasyonları dördüncü sırada bulunmaktadır. Veri gizliliği endişeleri ise %62 ile beşinci sırada gelmektedir [Strandell, 2024]. İngiltere'de yapılan diğer bir araştırma da, karantina sırasında enfeksiyon korkularını hedef alan dolandırıcılıkların, insanların %36'sını mağdur ettiğini ortaya koymaktadır [Safonov, 2022]. ABD'de ise Federal Ticaret Komisyonu'nun yayınladığı verilere göre tüketiciler 2023 yılında dolandırıcılıklar nedeniyle 10 milyar dolar kaybetti. Bu rakam, 2022'ye kıyasla 1 milyar dolar daha fazla olup, yeni bir rekora işaret etmektedir. Dolandırıcılık kategorileri arasında, suçluların devlet yetkilileri veya meşru işletmelerin temsilcileri gibi davrandığı kimlik hırsızlığı dolandırıcılıkları ilk sırada yer almaktadır [Delling, 2024].

Bu sorun günümüzde Kazakistan için de son derece önemlidir. Polisin verilerine göre, 2023 yılında Kazakistan vatandaşları dijital dolandırıcıların eylemleri nedeniyle 17,5 milyar tengeyi aşan zarara uğramıştır [Smagulov, 2023]. 2024 yılında ise 11,765 internet dolandırıcılığı vakası kaydedildi. Geçen yılın aynı dönemi ile kıyaslandığında vaka sayısında (152) artış olduğu görülmektedir [Kazakhstan Today, 2024].

Dijital suçlardan bazılarını ele alacak olursak bunlar temel olarak sosyal mühendislik, aldatma ve duygusal manipülasyon yoluyla bir kişinin davranışını etkilemeyi amaçlar. Dijital dünyada, siber suçlular insanları hassas bilgileri ifşa etmeye veya kendilerine veya işverenlerine mali zarar verebilecek eylemlerde bulunmaları yönünde kandırmak için sosyal mühendislik taktiklerini kullanırlar. Hatta seçimleri etkileyebilir veya finansal piyasaları manipüle edebilirler.

Oltalama (phishing), sosyal mühendislik taktiği olarak sahte e-postalar yoluyla alıcıları para göndermeye veya hassas bilgileri paylaşmaya yönlendirmeyi hedefler. Pek çok e-posta, alıcılardan bir bağlantıya tıklamalarını veya bir eki indirmelerini ister. Ancak bu tür eylemler, kötü amaçlı bir web sitesine yönlendirilmek, bir bilgisayar virüsünü çalıştırmak ya da tehlikeli bir yazılım indirmek gibi istenmeyen sonuçlara yol açabilir.

Hedefli oltalama (spear phishing), dolandırıcıların iletişime geçmeden önce araştırma yaptığı bir yöntemdir. Bu nedenle, kurbana adıyla hitap edebilir veya kurbanın tanıdığı bir kişi ya da şirketin temsilcisi gibi davranabilirler. Vishing, telefon görüşmeleri veya sesli mesajlar yoluyla yapılan bir oltalama türüdür; smishing ise SMS yoluyla gerçekleştirilir [Delling, 2024].

Yaşananlar, dolandırıcılık olaylarına karşı özel eğitim almış kişilerin dahi dolandırıcıların kurbanı olabileceğini göstermektedir. Örneğin, Hong Kong'da yakın zamanda yaşanan bir olayda, bir uluslararası finans hizmetleri şirketi 25,6 milyon dolar kaybetmiştir. Bir çalışan, şirketin CFO'su da dahil olmak üzere meslektaşları gibi görünen ve konuşan ancak aslında yapay zeka tarafından oluşturulan kişilerin yer aldığı sahte bir video konferansının ardından şirket fonlarını bir suç hesabına aktardı. Yapay zekanın, başkalarının ikna edici görüntülerini, videolarını veya seslerini üretme yeteneği, dijital suçlar için yeni fırsatlar yaratmaktadır [Chen ve Magramj, 2024]. Dijital suçlularla mücadele etmek için neler yapılabilir? Bazı uzmanlar, analitik düşünmenin sahte web sitelerine karşı direnç sağladığını [Shang ve diğerleri, 2023] ve bunun yanı sıra siber dayanıklılığı artırmak için sistematik eylemler gerektiğini düşünmektedir.

Mart 2023'te Kazak hükümeti, daha önce Kazakistan Siber Kalkanı programı çerçevesinde oluşturulan Ulusal Siber Güvenlik Koordinasyon Merkezi'ni daha da geliştirmeyi planlayan 2023-2029 için Dijital Dönüşüm, Bilgi ve İletişim Teknolojileri ve Siber Güvenlik Endüstrisinin Geliştirilmesi Konsepti'ni onayladı. Ayrıca, bilgi güvenliği uzmanlarının

Yazar: Prof. Dr. Gulnar NADIROVA
Avrasya Araştırma Enstitüsü, Kazakistan

eğitimi için bir siber eğitim sahası oluşturulması planlamaktadır [Avezova, 2024].

2024 yılında, 194 ülkenin siber saldırılara hazırlık seviyesini değerlendiren uluslararası sıralamaya göre, Kazakistan siber güvenlik alanında önemli bir ilerleme kaydederek beşinci seviyeden ikinci seviyeye yükseldi. Bu, siber güvenlik alanındaki güvenliğini başarılı bir şekilde geliştirmekte olduğunu doğrulamaktadır [The Tech, 2024]. Bilgi güvenliği ve kişisel veri koruma üzerine yapılan bir sosyolojik araştırma, Kazakistan nüfusunun %80,4'ünün mevcut siber güvenlik ve kişisel veri tehditlerinin farkında olduğunu ortaya koydu. Araştırmaya göre, katılımcıların %74,64'ü oltalama girişimlerini tanıyabilmekte; %90,52'si ise sosyal medyada kişisel bilgilerin nasıl korunacağını bilmektedir. Söz konusu sonuçlar, bu alanda kamu farkındalığını artırmada olumlu bir ilerleme sağlandığını göstermektedir.

Bununla birlikte, bu alandaki zorluklar, dijital çağda vatandaşların çıkarlarının sürdürülebilir bir şekilde korunmasını sağlamak için önlemlerin ve mekanizmaların sürekli olarak iyileştirilmesini gerektirmektedir. Genel olarak, araştırma bulguları, bilgi güvenliğinin Kazakistan vatandaşlarının günlük yaşamındaki artan önemini vurgulamaktadır. Bu bağlamda, gerçekleştirilen sosyolojik araştırmayı dikkate alarak, araştırma grubu vatandaşların güvenliğini sağlamak ve dijital alandaki verilerini korumak için ilgili tavsiyeler ve öneriler geliştirdi [gov.kz, 2023]. 11 Aralık 2023'te, kişisel verileri içeren kimlik belgelerinin kopyalarının toplanması ve işlenmesine yasal bir yasak getiren yeni bir koruma sistemi getirildi; Kazakistan Cumhuriyeti «Bilgilendirme Hakkında» kanun'un 56. maddesi uyarınca, bu bilgilere sahip olan kişiler, bu kanun uyarınca bunları korumak için önlemler almakla yükümlüdür [egov.kz, 2023].

Yasal çerçeveye ve hükümet önerilerine uymanın yanı sıra, bireyler veri güvenliği konusunda dikkatli ve proaktif olmalıdır. Alınması gereken başlıca adımlar şunlardır:

Bilgisayarları ve mobil cihazları güncel tutmak, her hesap için güçlü ve benzersiz parolalar kullanmak, bunları düzenli olarak güncellemek ve mümkün olan en uzun parolaları seçmek, dijital cihazları korumak için en etkili önlemlerden biridir. Bunların yanı sıra tüm hesaplarda ek bir güvenlik katmanı sağlamak için çok faktörlü kimlik doğrulamayı (MFA) etkinleştirmek; bağlantılara tıklarken, ekleri açarken veya hassas bilgileri paylaşırken dikkatli olmak; kredi kartı bilgileri gibi kişisel bilgileri girmeden önce web sitesinin HTTPS (buradaki «S» giriş yapılan sayfanın güvenli olduğu anlamına gelir) kullandığından emin olmak; verileri hem bilgisayarlarda hem de mobil cihazlarda yedeklemek; sadece güvenilir web sitelerinden alışveriş yapmak ve önce müşteri yorumlarını kontrol etmek; çocuklar ve diğer aile üyelerini çevrimiçi güvenlik hakkında bilgilendirmek; kişisel bilgileri ve finansal kayıtları kontrol altında tutmak, son olarak çevrimiçi hesaplarınızdaki gizlilik ayarlarını düzenli olarak gözden geçirerek kimlerin verilerinize erişebileceğini yönetmek ve olası dolandırıcılık girişimlerine derhal müdahale etmek gibi önlemleri almak gerekir.

Vatandaşlar, kısaca değindiğimiz bu önlemleri alarak dijital güvenliklerini korumada aktif bir rol alabilirler. Diğer taraftan hem küresel hem de ulusal düzeyde artan

dijital suçlara karşı korunabilmenin kapsamlı bir yaklaşım gerektirdiği tartışmasızdır. Kısaca, hükümet tedbirlerini, eğitim girişimlerini ve vatandaşların kişisel sorumluluklarını birlikte ele almak önemlidir. Yalnızca bu şekilde yüksek teknoloji çağında sürdürülebilirlik ve dijital tehditlere karşı koruma sağlanabilir.

Kaynakça:

Avezova, Yana (2024). BDT ülkelerindeki güncel siber tehditler 2023-2024. Alınan yer: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/#id6. Erişim tarihi: 17.12.2024.

Chen, Heather and Kathleen, Magramo (2024). Finans çalışanı, deepfake 'finans müdürü' ile yaptığı görüntülü görüşmenin ardından 25 milyon dolar ödedi. Alınan yer: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html#:~:text=A%20finance%20worker%20at%20a,according%20to%20Hong%20Kong%20police. Erişim tarihi: 22.12.2024.

Delling, Dianna (2024). Dolandırıcılık önleme. Sosyal mühendislik dolandırıcılıklarını ve siber tehditleri tespit etme rehberiniz. Alınan yer: https://newsroom.mastercard.com/news/perspectives/2024/your-guide-to-identifying-social-engineering-scams-and-cyber-threats/. Erişim tarihi: 11.12.2024.

Egov.kz (2023). Siber güvenlik sorunları. Alınan yer: https://egov.kz/cms/sites/default/files/rekomendacii_2023.pdf. Erişim tarihi: 11.12.2024.

Kazakhstan today (2024). Kazakistan'da internet dolandırıcılığı vakalarının sayısı arttı. Alınan yer: https://www.kt.kz/rus/crime/v_kazahstane_vozroslo_kolichestvo_faktov_1377968514. Erişim tarihi: 12.12.2024.

Safonov, Vladimir and Andreev, Dmitri (2022). «Pandemi Dolandırıcılığı»: Hırsızlığın Yeni Yolları. V.N. Tatishchev Adlı Volga Üniversitesi Bülteni, vol.1, № 2 (101), 177-184. Alınan yer: https://cyberleninka.ru/article/n/moshennichestvo-ot-pandemii-novye-sposoby-hischeniy Erişim tarihi: 12.12.2024.

Shang, Yuxi, Wang, Kaije, Tian, Yuye, Zhou, Yingyu, Ma, Beibei ve Liu, Sanyang (2023). İnternet dolandırıcılığı mağduriyetinin teorik temeli ve oluşumu: Karar alma ve muhakemede iki sisteme dayanmaktadır. Alınan yer: https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1087463/full Erişim tarihi: 11.12.2024.

Smagulov, Aset (2024). Kazakistan'da çevrimiçi dolandırıcılık vakalarının sayısı son yedi yılda on kat arttı. Alınan yer: https://ulysmedia.kz/news/24758-v-desiat-raz-vozroslo-kolichestvo-internet-moshennichestva-v-kazakhstane-za-poslednie-sem-let/. Erişim tarihi: 11.12.2024.

Strandell, Jonas (2024). Çevrimiçi dolandırıcılıkların evrimi. Alınan yer: https://besedo.com/blog/the-evolution-of-online-scams-moderation-methods/ Erişim tarihi: 11.12.2024.

The Tech (2024). Kazakistan, 2024 küresel siber güvenlik sıralamasındaki konumunu güçlendiriyor. Alınan yer: https://the-tech.kz/kazahstan-ukrepil-poziczii-v-globalnom-rejtinge-kiberbezopasnosti-2024/#:~:text=%. Erişim tarihi: 22.12.2024.