Hacking’i Anlamak: Türler, Yöntemler, Motivasyonlar ve Hukuki Sonuçlar

Ahsen Beyza Özkul

ahsenbeyza@securedebug.com

İÇİNDEKİLER

Giriş

Hacking, dijital sistemlere izinsiz erişim sağlama veya bilgileri manipüle etme eylemidir. Bazı hackerlar, "etik hackerlar" olarak bilinir ve güvenliği artırmak için çalışırken, diğerleri yasa dışı faaliyetlerde bulunur ve bu durum ciddi zararlar verebilir. Bu yazı, hacking'in ne olduğunu, hackerların kimler olduğunu, motivasyonlarını, kullandıkları yaygın yöntemleri ve bu faaliyetleri ele alan hukuki çerçeveyi incelemektedir. Bu unsurları anlamak, hacking'in dijital dünyamız üzerindeki etkilerini daha iyi kavrayabilmemizi sağlar.

Hacking Nedir ve Hackerlar Kimlerdir?

Hacking, dijital cihazlarda, ağlarda veya sistemlerdeki güvenlik açıklarını kullanarak izinsiz erişim sağlama veya yetkisiz eylemler gerçekleştirme işlemidir. Hacking meşru amaçlarla, örneğin güvenlik açıklarını tespit edip düzeltmek için yapılabilir (bu tür hackerlar "etik hacker" olarak bilinir), ancak genellikle yasa dışı faaliyetlerle ilişkilendirilir. Siber güvenlik alanında, hacking genellikle bilgisayarlar, akıllı telefonlar, tabletler veya ağlar gibi cihazları tehlikeye atmayı, bilgi çalmayı veya operasyonları aksatmayı içerir.

Hackerlar, bu faaliyetleri gerçekleştiren kişilerdir. İlk başlarda, hackerlar yazılım veya elektronik sistemleri keşfetmek ve nasıl çalıştığını anlamak için eğlenen kişiler olarak görülüyordu. Bu tür hackerlar "beyaz şapka" hackerlar olarak adlandırılır ve becerilerini güvenliği artırmak veya teknik sorunları çözmek için kullanırlar.

Zamanla, "hacker" terimi kötü niyetli faaliyetlerde bulunan kişileri tanımlamak için de kullanılmaya başlandı. Bu kişiler "siyah şapka" hackerlar olarak bilinir ve sistemlere girerek veri çalma, zarar verme veya kişisel kazanç sağlama amacı güderler. Sistemlerdeki zayıflıkları kullanarak veri ihlalleri, kimlik hırsızlığı ve finansal kayıplara yol açarlar.

Ayrıca, "gri şapka" hackerlar da vardır. Bu kişiler izinsiz olarak sistemlere erişebilir ancak kötü niyetli bir amacı yoktur; genellikle güvenlik açıklarını vurgularlar ve bazen bunları düzeltmeye çalışırlar, ancak resmi yetki olmadan bunu yaparlar.

Artık hacking oldukça sofistike ve karlı bir endüstri haline gelmiştir. Siber suçlular, genellikle organize gruplar halinde çalışarak gelişmiş tekniklerle sistemlere sızar, hassas bilgileri çalar ve tespit edilmekten kaçınırlar.

Hacking'in Tarihi

Hacking'in tarihi, birkaç on yıl içinde önemli ölçüde değişmiştir; bu süreç yaratıcı problem çözme faaliyetlerinden büyük bir siber güvenlik endişesine dönüşmüştür.

1950’ler ve 1960’larda "hacking", MIT’de teknolojiyle oynama anlamında kullanılıyordu; öğrenciler model trenlerle ve sonunda bilgisayarlarla deneyler yapıyordu.
1970’lerde, hacking “telefon phreaking” ile yeni bir yön aldı; hackerlar telefon sistemlerini sömürerek ücretsiz aramalar yapıyorlardı ve bu durum teknik açıkların nasıl kullanılabileceğini gösteriyordu.

1980’ler, kişisel bilgisayarların ön plana çıkmasıyla hacking’i kamuoyuna tanıttı, özellikle "WarGames" filmi bir gencin askeri sistemlere kazara sızmasını konu aldı. Bu dönem, ilk hacker gruplarını gördü ve ABD hükümetinin 1986’da Bilgisayar Dolandırıcılığı ve Kötüye Kullanım Yasası’nı çıkarmasına neden oldu; bu yasa izinsiz bilgisayar erişimini yasa dışı kılmaktadır.

1990’larda, internetin yükselmesi hacking fırsatlarını artırdı. "Beyaz şapka" hackerlar güvenliği artırmaya çalışırken, "siyah şapka" hackerlar sistem açıklarını kişisel kazanç sağlamak için kullandılar. "Hacktivizm" de ortaya çıktı; bu hackerlar siyasi nedenleri teşvik etmek için yeteneklerini kullandılar ve hükümetleri veya karşı oldukları şirketleri hedef aldılar.

2000’lerde, internetin günlük yaşamın bir parçası haline gelmesiyle siber güvenlik öncelik haline geldi. Şirketler, artan tehditlerden korunmak için etik hackerları işe almaya başladı.

2010’lardan itibaren, hacking devlet destekli faaliyetler için bir araç haline geldi ve hükümetlere ve şirketlere yönelik sofistike siber saldırılar gerçekleştirildi.

Siyah Hacker’ların Motivasyonları

Hackerlar birkaç temel faktörden motive olabilirler:

1) Para: Birçok hacker, finansal bilgileri çalarak, fidye yazılımları saldırıları başlatarak veya çalınan verileri satarak hızlı para kazanmayı hedefler.

2) İntikam: Kötü deneyim yaşayan bireyler, genellikle eski çalışanlar, kendilerini yanlış bulan organizasyonlara karşı hack yaparlar.

3) Siyasi İnançlar: Hacktivistler, siyasi veya sosyal nedenleri teşvik etmek için hack yaparlar ve karşı oldukları hükümetleri veya şirketleri hedef alırlar.

4) Merak ve Zorluk: Bazı hackerlar, güvenlik sistemlerini aşmanın ve becerilerini kanıtlamanın heyecanıyla motive olurlar.

5) Ün: Bazıları, hacker topluluğunda tanınmak için yüksek profilli saldırılar gerçekleştirmeyi hedefler.

6) Casusluk: Devlet destekli veya kurumsal hackerlar, stratejik veya rekabetçi avantajlar elde etmek için hassas bilgileri hedef alırlar.

Yaygın Hacking Yöntemleri

Siyah şapka hackerlar, sistemlere sızmak ve bilgi çalmak için çeşitli yöntemler kullanır. İşte en yaygın tekniklerden bazıları:

1) Sosyal Mühendislik: Hackerlar, IT destek veya tedarikçiler gibi güvenilir biri gibi davranarak insanları hassas bilgileri açıklamaya ikna ederler. Şifre bilgilerini almak için phishing e-postaları gönderebilirler ve bu bilgileri kullanarak sistemlere ve verilere erişebilirler.

2) Kod Enjeksiyonu: Bu teknik, bir sistemin girdi verilerini düzgün şekilde kontrol etmediği yerlerde zararlı kod eklemeyi içerir. İçeri girdikten sonra, saldırgan sistemi kontrol edebilir, veri çalabilir veya diğer saldırılar başlatabilir. Yaygın bir örnek SQL enjeksiyonudur; hackerlar, web sitesi açıklarını kullanarak veritabanı bilgilerine erişirler.

3) Cross-Site Scripting (XSS): Hackerlar, meşru web sitelerine zararlı kod enjekte eder. Kullanıcılar bu siteleri ziyaret ettiğinde, saldırgan kişisel verilerini çalabilir. XSS saldırıları "depolanmış" (sunucuda kalıcı) veya "yansıtılmış" (kullanıcıya, meşru gibi görünen bir şekilde geri döner) olabilir.

4) Kaba Güç Saldırıları: Hackerlar, doğru şifreyi bulana kadar farklı şifre kombinasyonlarını tekrar tekrar denerler. Bu yöntem basittir ancak şifrenin karmaşıklığına bağlı olarak çok fazla işlem gücü gerektirir.

5) Çerezler: Web siteleri tarama sırasında bilgisayarınıza çerezler kaydeder; bu çerezler, oturum açma bilgileri gibi hassas veriler içerebilir. Eğer hackerlar bu çerezleri çalarsa, sizi çevrimiçi olarak taklit edebilir veya hesaplarınıza erişebilirler.

Hukuki Çerçeve: Siyah Şapka ve Beyaz Şapka Hackerlar

Siyah şapka hackerlar yasa dışı faaliyetlerde bulunur. Yasalar ve düzenlemelerin siyah şapka hackerlarına bazı etkileri olur.

1) Bilgisayar Dolandırıcılığı ve Kötüye Kullanım Yasası (CFAA) - ABD: Bilgisayarlara izinsiz erişimi suç sayar. Siyah şapka hackerlar sistemlere girip veri çaldığında bu yasayı ihlal ederler.

2) Dijital Milenyum Telif Hakkı Yasası (DMCA) - ABD: Telif hakkıyla korunan materyalleri korur. Siyah şapka hackerlar korsan içerik dağıttıklarında bu yasayı çiğnerler.

3) Genel Veri Koruma Yönetmeliği (GDPR) - AB: Kişisel verileri korur. Siyah şapka hackerlar AB vatandaşlarının kişisel bilgilerini çaldığında GDPR kapsamında ağır cezalara çarptırılırlar.
4) Siber Güvenlik Bilgi Paylaşımı Yasası (CISA) - ABD: Siber güvenlik bilgilerini paylaşmayı teşvik eder. Siyah şapka hackerlar açıkları rapor etmeden sömürdüklerinde, bu paylaşımın zorlaştırılmasına neden olurlar.

5) Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) - ABD: Sağlık bilgilerinin korunmasını sağlar. Siyah şapka hackerlar tıbbi kayıtları hedef aldıklarında HIPAA'yı ihlal ederler.

Beyaz şapka hackerlar becerilerini yasal yollarla güvenliği artırmak için kullanır. İşte yasaların onları nasıl desteklediği:

1) Bilgisayar Dolandırıcılığı ve Kötüye Kullanım Yasası (CFAA) - ABD: Beyaz şapka hackerlar sistemleri test etmek için izin almalıdır. Yasalara uyarak ve yetki alarak test ettiklerinde cezalandırılmazlar.

2) Siber Güvenlik Bilgi Paylaşımı Yasası (CISA) - ABD: Beyaz şapka hackerlar, güvenlik açıkları hakkında bilgi paylaşarak yardımcı olurlar. CISA, tehditleri rapor edenleri korur.

3) Ağ ve Bilgi Sistemleri Direktifi (NIS Direktifi) - AB: Beyaz şapka hackerlar, NIS gereksinimlerini karşılamak için açıkları tespit edip rapor ederek katkıda bulunurlar.

Kaynaklar

1) Birleşmiş Milletler Uyuşturucu ve Suç Ofisi. (2019, Şubat). *Siber suç yasalarının rolü*. Birleşmiş Milletler Uyuşturucu ve Suç Ofisi. https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html
2) Sovandeb. (2023, 27 Haziran). *Web sitesi hackleme teknikleri*. Astra. https://www.getastra.com/blog/knowledge-base/website-hacking-techniques/
3) Blue Team Alpha. (2022, 21 Temmuz). *Bir hacker'ı motive eden nedir*. Gradient Cyber. https://www.gradientcyber.com/resources/what-motivates-a-hacker
4) Morpus, N. (2022, 26 Temmuz). *Hackleme yöntemleri ve motivasyonları nelerdir*. VMware. https://blogs.vmware.com/security/2022/07/what-are-the-methods-and-motives-for-hacking.html
5) BRANDEFENSE. (2023, 24 Ekim). *Siber saldırılar: Hacker'ları motive eden nedir*. Brandefense. https://brandefense.io/blog/drps/cyberattacks-what-motivates-hackers/
6) Proofpoint. (t.y.). *Hackleme*. https://www.proofpoint.com/au/threat-reference/hacking
7) Cybersec Talent. (2024, 28 Mart). *Hacklemenin tarihi*. https://cybersectalent.co.uk/the-history-of-hacking/
8) Fortinet. (2023). *Hackleme nedir*. *Küresel Tehdit Manzara Raporu 2Y 2023*. https://www.fortinet.com/resources/cyberglossary/what-is-hacking
9) Malwarebytes. (t.y.). *Hacker*. https://www.malwarebytes.com/cybersecurity/basics/hacker
10) Imperva. (t.y.). *Sistem hackleme*. https://www.imperva.com/learn/application-security/system-hacking/