Cybercrime, Cybersecurity und Digitale Forensik

Von EKHK Christian Zwick, Ludwigshafen

Die Bedrohungsanalysen renommierter Sicherheitsdienstleister stellen seit Jahren eine zunehmende Vielfalt an Schadsoftware und ein kontinuierliches Wachstum von Cyberangriffen fest. Einige Attacken können abgewehrt werden, dennoch fallen nach und nach verschiedenste Unternehmen, Einrichtungen und Behörden den Cyberkriminellen zum Opfer. Die COVID-19-Pandemie scheint diese Kriminalitätsform noch anzustacheln. Aufgrund der zunehmenden Bedeutung für die polizeiliche Praxis werden im Folgenden einige Fachbegriffe zu diesem Kriminalitätsfeld erläutert.

Cybercrime

Unter Cybercrime (dt. Computerkriminalität) versteht man diejenigen Straftaten, bei deren Begehung die Kriminellen moderne Informations- und Kommunikationstechnik verwenden bzw. diese als Werkzeuge oder als Tatobjekt nutzen. Cybercrime *im weiteren Sinne* meint Taten aus nahezu allen Deliktsgruppen, bei denen Computer bzw. IT-Systeme zur Planung, Vorbereitung oder Ausführung eingesetzt werden (z.B. Urheberrechtsverletzungen, Verbreitung von Kinderpornografie, Hasskriminalität oder Cybergrooming). Cybercrime *im engeren Sinne* umfasst diejenigen Tatbestände des StGB, welche eigene IT-Merkmale wie beispielsweise *„Datenerlangung“, „Datenmanipulation“* oder die *„Veränderung eines Programms“* enthalten. Dazu gehören u.a. die Straftaten in den §§ 202a-d (Ausspähen und Abfangen von Daten etc.), 303b (Computersabotage) oder 263a StGB (Computerbetrug).

Cybersecurity

Über die Reichweite des Begriffs Cybersecurity ist man sich in der Fachweltnicht einig. Die Wortbedeutung des Duden und das Attribut *„Cyber“* legen nahe, dass diese sich auf ein bestimmtes Handlungsfeld der IT-Sicherheit bezieht, nämlich auf den Schutz vor kriminellen Aktivitäten und vorsätzlichen Handlungen. Unfälle oder höhere Gewalt wären demzufolge nicht erfasst. Allerdings, nach dem BSI Standard 200-1, wird das Aktionsfeld der klassischen IT-Sicherheit unter dem Begriff *„Cyber-Sicherheit“* auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.[2]

Digitale Forensik

Zum Begriff der IT-Forensik hat sich bislang keine eindeutige Definition durchgesetzt. Laut dem Leitfaden IT-Forensik v1.0.1 des BSI (aus dem Jahre 2011) ist *„IT-Forensik die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.“*[3] Dabei unterscheidet man in Online-Forensik (*„live“*, am aktiven System) und Offline-Forensik (*„post-mortem“,* nach Deaktivierung der Stromversorgung). Letztere erfolgt u.a. mithilfe von 1:1 Kopien des Speichers bzw. Datenträgerabbildern. Grundlegende Anforderungen sind insbesondere die lückenlose Beweiskette (*„Chain-of-Custody“*), die Integrität der Asservate sowie das systematische Vorgehen unter Nutzung anerkannter Methoden und Werkzeuge.

Advanced Persistent Threat (APT)

Wie das Adjektiv *„advanced“* bereits vermuten lässt, kommen bei einer *„hochentwickelten, hartnäckigen Bedrohung“* kontinuierlich und heimlich angewendete, ausgeklügelte Hackertechniken zum Einsatz, die den Zugang zu einem System ermöglichen und dafür sorgen, dass Hacker über einen längeren Zeitraum im System verbleiben und dort Schaden anrichten

können. Aufgrund des für einen solchen Angriff erforderlichen Aufwands richten sich APTs in der Regel gegen gewichtige Ziele, wie etwa Nationalstaaten und Großunternehmen.[4]

Darknet

Nur ein Teil des Internetverkehrs ist für die meisten Nutzer überhaupt sichtbar und als das bekannt, was wir als Internet kennen. Suchmaschinen wie Bing oder Google können demnach nur indizieren, was auch als Teil des sichtbaren Internets über die herkömmlichen Dienste und Protokolle zu erreichen ist. Über die Infrastruktur des Internets werden zudem andere Netze als *„Overlay-Netzwerke“* abgebildet, welche das Internet nur als Transportschicht verwenden. Der größere, nicht sichtbare Teil des Internets wird daher als Deep Web bezeichnet. Hier tummeln sich spezielle Forschungsnetze, Peer-to-Peer-Tauschbörsen wie BitTorrent und auch das Tor-Netzwerk, welches landläufig als *„Darknet“* oder *„dunkles Internet“* bezeichnet wird. Der Umfang des Deep Webs ist viel größer als der des sichtbaren Internets.[5]

Exploits

Exploits sind kleine Programme, die Sicherheitslücken auf dem Computer ausfindig machen und ausnutzen. Die eigentliche Schadsoftware, zum Beispiel Ransomware, wird meist erst später nachgeladen. Exploits verbreiten sich meist auf zwei Arten. Im ersten Fall werden sie beim Surfen im Internet unbemerkt mit den anderen Inhalten der Webseite heruntergeladen. Im zweiten Fall verbergen sie sich in Dateien im Anhang von E-Mails, auf USB-Sticks, externen Festplatten und ähnlichem.[6]Zu bekannten Exploits werden Listen veröffentlicht, beispielsweise unter www.exploit-db.com.

Lateral Movement

Das *„Lateral Movement“* (dt. seitliche Bewegung in Netzwerken) wird von Angreifern verwendet, um über bereits gekaperte gewöhnliche Nutzerrechte die wirklich sensiblen Konten und Computer im Netzwerk zu identifizieren und über diese schließlich auf (i.d.R. codiert) gespeicherte Anmeldeinformationen zuzugreifen. Im Erfolgsfalle kann ein Angreifer sogar Zugriff auf den Domänencontroller erhalten.[7] Damit erlangt er Admin-Rechte auf allen Computern im Netzwerk.

OSINT

Open Source Intelligence (OSINT) ist ein Begriff aus der Welt der Nachrichtendienste, bei dem für die Nachrichtengewinnung Informationen aus frei verfügbaren, offenen Quellen gesammelt werden, um durch Analyse der unterschiedlichen Informationen verwertbare Erkenntnisse zu gewinnen. Dabei werden frei zugängliche Massenmedien genutzt, wie die Printmedien mit Zeitschriften, Tageszeitungen sowie Radio und Fernsehen, aber auch das Internet (speziell Soziale Medien) und Web-basierte Anwendungen wie Google Earth. Damit die zahlreichen *„Informationsschnipsel“* zu einem Erkenntnisgewinn führen, müssen diese nach ihrer Beschaffung zusammengesetzt und analysiert werden, um daraus das gewünschte *„Informationsprodukt“* aufzubauen.[8] Eine Übersicht zu gängigen Tools findet man unter https://osintframework.com/.

Privilege Escalation

Als Rechteausweitung, auch Rechteerhöhung, Privilegien-Erweiterung oder Privilegien-Eskalation genannt, bezeichnet man die Ausnutzung eines Computerbugs bzw. eines Konstruktions- oder Konfigurationsfehlers einer Software (Vulnerability) mit dem Ziel, einem Benutzer (hier: einem Angreifer) oder einer Anwendung Zugang zu Ressourcen zu verschaffen, deren Nutzung mit eingeschränkten Rechten nicht möglich ist.[9]

Vulnerability

Eine Vulnerability bedeutet eine Sicherheitslücke bzw. Schwachstelle in einer Anwendung, einem IT-System oder einem Netzwerk. Diese kann durch Angreifer u.a. mit schädlichem Programmcode (vgl. *Exploits*) ausgenutzt werden, um unerlaubt Zugriff auf digitale Ressourcen zu erhalten. Erkannte und bestätigte Schwachstellen werden durch internationale Institutionen i.d.R. veröffentlicht. Die Die *„Common Vulnerabilities and Exposures“* (dt. häufige Schwachstellen und Risiken) ist eine standardisierte Namenskonvention bzw. eine öffentliche Liste zu Sicherheitsschwachstellen in Computersystemen (siehe nvd.nist.gov/vuln). [10]

Anmerkungen

1. Christian Zwick ist Erster Kriminalhauptkommissar, Leiter des Kommissariats 16 (IT-Forensik/Technische Ermittlungsunterstützung) der ZKI Ludwigshafen und Mitglied des Redaktionsteams dieser Zeitschrift.
2. Vgl. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.pdf.

3. Vgl. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf.
4. Mehr: www.kaspersky.de/resource-center/definitions/advanced-persistent-threats.
5. Vgl. www.wintotal.de/darknet-zugang.
6. Vgl. www.gdata.de/ratgeber/was-ist-eigentlich-ein-exploit.
7. Übersetzt aus docs.microsoft.com/en-us/azure-advanced-threat-protection/use-case-lateral-movement-path.
8. Vgl. de.wikipedia.org/wiki/Open_Source_Intelligence.
9. Vgl. de.wikipedia.org/wiki/Rechteausweitung.
10. Vgl. www.redhat.com/de/topics/security/what-is-cve.