Vortrag

Cyberwar

apl. Prof. Dr. Dr. Saalbach Mai 2019

Themen

-Was versteht man unter Cyberwar?

-Wie und womit wird angegriffen?

-Wer greift an und warum?

-Wie erkennt man die Angreifer?

-Wie kann man sich schützen?

-Welche Rolle spielt die Smart Industry (Industrie 4.0)?

Was ist Cyberwar?

-kriegerische Auseinandersetzung mit den Mitteln der Informationstechnologie

-integriertes und unterstützendes Element konventionellen militärischen Handelns

-Zusammenspiel von Mensch und Maschine

-Computer/Digitaltechnologie als Werkzeug

-Offensiv und defensiv: eigene Spielräume sichern und erweitern, die des Gegners begrenzen

-Im Kriegsfall Cyberattacken/physische Angriffe zeitlich eng verknüpft

Cyberwar in der Praxis

-Ausschaltung der gegnerischen Luftabwehr (2007)

-Sabotage von Uranzentrifugen (2010)

-Infiltration und Spoofing von Kampfdrohnen (2011/2012)

-Lahmlegen von kritischen Infrastrukturen (Saglam-Studie 2014/Ukraine 2015)

-Cyberwar gegen den Islamischen Staat (2016)

-Ausbau der Cyberwarkapazitäten (GB, F, Science Squadrons, CNO…)

-Verlegung russischer Cybersoldaten nach Venezuela (2019)

Spionage und Cyberwar

-Cyberattacken erfordern das Eindringen in digitale Geräte
Hacker > Intrusion > Malware >Aktion > zweigleisige Kommunikation zwischen infiziertem Gerät und Angreifer

-Ziele sind Spionage, Manipulation, Sabotage, Diebstahl/Erpressung und Missbrauch

-Die Grenzen zwischen Spionage und Cyberwar sind fließend, da der Cyberwar in der Regel die Intrusion voraussetzt

-Auch in der Spionage kann der Computer den Agenten vor Ort nur ergänzen, aber nicht ersetzen

Cyberattacken

Aktuell führende Methoden:

- Emails mit malignen Anhängen oder Links (Phishing) mit Social Engineering
- Exploits (Schwachstellen, Backdoors und Bugdoors)
- Infizierte Apps und Websites
- Insider-Threats am gefährlichsten
- Botnetze: Nutzung von infizierten digitalen Geräten als ‚bots', um einen Zielcomputer mit Daten bzw. Anfragen zu überfluten und lahmzulegen (Distributed Denial of Service DDoS).

Cyberwaffen

Programme, mit denen man andere Computer angreifen, infiltrieren, ausspionieren und manipulieren kann und die ggf. ihre Ausbreitung und Abschaltung selbsttätig steuern können.

Klassisch: Viren (die sich im Computer festsetzen),
Trojaner (die Vorgänge auf dem Computer nach draußen melden) und
Würmer (die sich selbsttätig im Netz verbreiten können)

Modern: beachheads, modular, variabel, maßgeschneidert, ständige Updates, ‚stealthy' = schwer zu erkennen und zu löschen, Verschleierung und false flags

Offensive Cyberwaffen:
falsche Signale (GPS, Täuschkörper, 20 kHz-Befehle), Botnetze, logische Bomben, Textbomben, Wiper-Malware, Bricking, Ransomware, Fuzzing

Offensive Cyberwaffen

Was?	Wofür?
falsche Signale	GPS Spoofing: Irreführung von Drohnen, Schiffen etc.
	Täuschkörper: Attrappen zur Irreleitung autonomer Systeme, neue Form der Tarnbemalung mit großen kontrastarmen Pixeln
	20 kHz-Befehle: Ultraschallbefehle zur Fern-Manipulation von Heimlautsprechern
Botnetze	Überflutung mit Anfragen und Daten kann Computer bzw. Netzwerke lahmlegen
logische Bomben	Schadprogramme, die erst nach einer bestimmten Zeit oder bestimmten Handlung aktiv werden
Textbomben	Schwer zu interpretierende Symbole, die den Chip überlasten und zum Absturz bringen
Wiper-Malware	Löschprogramme, die Dateien des infizierten Computers löschen
Bricking	Programme, die bei smarten Geräten wichtige Steuerdateien mit Nullen überschreiben und so das Gerät unbrauchbar machen
Ransomware	Sperrbildschirme, für deren Entsperrung Geld verlangt wird (Ransom=Erpressung): Immer häufiger als destruktive Ransomware, d.h. der Bildschirm lässt sich gar nicht mehr entsperren
Fuzzing	Zufallskommandos an Chips, die diesen aufgrund von Designlücken zur Datenfreigabe bringen oder gar endgültig anschalten (halt and catch fire)
	=> digitaler Rettungsschuss ist technisch möglich, latente Gefahr der ‚Abschaltung' durch Gegner im Gefechtsfall

Expansion der Angriffsziele

Früher	Heute
Computer	Zubehör: Maus, Drucker, Router, USB-Sticks Smartphones/iPhones Smart home: Internet der Dinge Infrastruktur: Zugang zu nationalen Servern, Anzapfen von Internetknoten, Umleitung und Kopieren des Datenverkehrs, Tiefseekabel anzapfen, Attacken auf Clouds, 5G-Sendemasten
Software	Hardware (Fuzzing), Firmware, Add-on Chips
Hacken/Virus	Interdiction (Abfangen), Diebstahl, ‚Virus ab Werk'
User	Datensammlung auf Vorrat („alles von allen")
	Höhere Ebenen: Bankkunden > Bank > Interbankensystem
	Attacken auf Drittfirmen, Zulieferer und Wartungssysteme, Help Desks und Vertragsmitarbeiter

Angreifer (I)

Hacker sind (noch) überwiegend männlich, jung, arbeiten mehrheitlich in Organisationen und nicht (mehr) als Einzelpersonen

Sektoren:

- Staat mit Zivilbehörden, Militär- und Geheimdiensten
- Privatwirtschaft mit Cybersicherheitsfirmen und Cyberwaffenproduzenten
- Wissenschaft (Forschung, Hochschulen)
- Cyberkriminelle (Darknet, Hackerforen, Schwarzmarkt)
- Politisch aktive Hacktivisten

Angreifer (II)

Advanced Persistent Threat (APT):
fortschrittliche anhaltende Bedrohung

Klassische Definition:

längerfristig agierende Angreifergruppen mit definierten Techniken, Taktiken und Programmen (TTPs)

Moderne Definition (für Spionage und Cyberwar):

Projektgruppe innerhalb eines Nachrichtendienstes, die ihre Techniken, Taktiken und Programme (TTPs) sowie die Angriffsziele entlang der operativen Vorgaben ihres Dienstes entwickelt und anwendet

Führende APTs

Land	Zuordnungen durch führende Cybersicherheitsfirmen
Russland	APT28/FancyBears/Sofacy/Strontium/Sednit (GRU)
	APT 29/Cozy Bears/Dukes (FSB oder SWR)
	Waterbug/Turla/Ouroburos/Venomous Bear/Krypton Gruppe (FSB)
	Sandworm/Quedagh (GRU)
	Energetic Bear/Dragonfly (unklar)
	Trisis/Triton/Temp Veles (Central Scientific Research Institute of Chemistry and Mechanics)
China (ca. 20 APTs)	APT 1/Comment Group (PLA)
	APT 10/Cloud Hopper (MSS)
USA	Equation Group (NSA)
	Longhorn/The Lamberts (CIA)
Nordkorea	Lazarus-Gruppe und Ableger
Israel	Unit 8200 (IDF)

Die genannten Staaten kommentieren diese Zuordnungen nicht bzw. dementieren sie.

Details und Quellen in: Cyberwar – Grundlagen Methoden Beispiele 2019

Attribution: Wer war es?

- Infrastruktur: IP-Adressen, Domain Names und Provider müssen angemeldet werden (Suche mit WHOIS etc.), Infrastrukturen und Namen werden oft recycelt
- Hacker: agieren in Foren, begrenzte Zahl von Decknamen
- Malware: eingebettet in andere Aktivitäten, Kopieren daher riskant
- Konventionelle Spionage/Gegenspionage: z.B. IP-Adressen kaufen, Überwachungskameras infiltrieren, in gegnerisches System einhacken usw.

Cyberverteidigung

Ebene	Verfahren
User	Regelmäßige Updates, vorsichtiger Umgang mit Dateien, Virenschutz, Spamfilter, sichere Passwörter, 2 Faktor-Authentisierung mit Passwort und einem Gegenstand, Daten verschlüsseln, Firewalls (Kontrolle des Netzwerkzugriffs) Forschung: Tastendruckdauer- und stärke sowie Mausbewegungsmuster als nicht imitierbare individuelle Kennungen
Organisation	Whitelisting, segmentierte Netze, Need to know, Vier Augen-Prinzip für Administratoren
Sicherheitsfirmen	Threat Intelligence, Intrusion Detection, Penetration Testing, Honeypots, Sandbox Analysis, Datenkombination
Kooperationen	Nachrichtendienste (z.B. 5-/9-/14-eyes), Polizei (Europol), ENISA, AK KRITIS, Charter of Trust usw…
Recht	Straf- und Haftungsvorschriften, Sicherheitsstandards
Technik	z.B. DDoS-Abwehr: Daten ableiten, Provider einschalten, eigene IP abschalten, fremde IP sperren (geoblocking), Verlangsamung (tarpitting) Einbahnstraßentechnologien: Campusnetzwerke (Daten raus, aber nicht rein), Datendioden (rein, aber nicht raus)

Smart Industry – Worum geht es?

- Smart Industry (Industrie 4.0): Digitalisiert (vernetzt, computerisiert, intelligent), u.a. mit Fernwartungs- und –Steuerungssystemen (Industrial Control Systems ICS/Supervisory Control and Data Acquisition SCADA)
- Teilgebiet der smarten Technologien (smart home, smart cities, smart grid/smart meter, smart cars usw.) und des Internets der Dinge (Internet of Things IoT)
- Ein Schlüsselelement wird die 5G-Technologie sein
- Exponentielles Wachstum von Geräten, Schnittstellen, Updates, Varianten
- Vernetzte = Offene Systeme: Monitoring, Wartung, Updates, Backdoors
- Geringer Passwortschutz/Unnötige Vernetzung: Shodan

Smart Industry Attacken

Grundlagen:

- Infiltration > lateral movement > Eskalation > Manipulation
- Entwicklung des Angriffs dauert Jahre (inkl. Tests) und erfordert die Zusammenarbeit von Informatikern und Ingenieuren
- Hacken allein reicht nicht, man muss auch das System genau kennen (sonst Entdeckung, versehentliche Sabotage)
- In der Regel wird nur spioniert, nicht sabotiert
  (im Cybercrime jedoch Ransomware und Botnetze)
- Das Primärziel ist die (Industrie)Spionage, der Cyberwar eine Option

Wichtige Attacken I

Stuxnet (2005-2010): Erst Lüftungsklappen, dann Frequenzen von Uranzentrifugen durch gezielte Attacke auf Simatic S7-SPS und die Prozessvisualisierung WinCC

Immer noch ungeklärt: Shamon-Attacke auf Aramco (2012), Wiper-Attacke auf den Iran 2012

Cloud Hopper (2006-2016): Angriff auf Managed Service Providers MSPs (Clouds, IT Services, Help Desks etc.), daneben auf Technologiefirmen und die US Navy

Lazarus-Gruppe (2012-heute): Seit Jahren Angriffe mit Wipern als logische Bomben oder zur Spurenverwischung, Einsatz destruktiver Ransomware (WannaCry) 2017

Triton/Trisis/Temp.Veles (2017): Malware Triton/Trisis gegen Schneider Electrics Triconex Safety Instrumented System (SIS) in Saudi-Arabien, Manipulation von Notabschaltungen

Dragonfly/Energetic Bear: infiziert Anbieter von ICS-Programmen mit Malware Havex zur Überwachung und Manipulation von ICS/SCADA-Systemen (ca. 2000 Fälle)/
Wolf Creek-Vorfall 2017 durch Spearphishing mit falschen Lebensläufen

Wichtige Attacken II

Sandworm/Quedagh (seit 2011): Modifizierte multifunktionale Malware BlackEnergy3 gegen vernetzte Benutzerschnittstellen (Human-Machine-Interfaces HMI)

2015 Stromausfälle in der Ukraine durch Trennen von Stromverbindungen mit Telephone Denial of Service (TDoS)-Angriffen zur Hotline-Blockade und Wipern (Killdisk)

2016 Industroyer-Angriff Falsche IEC-104 Protokollbefehle an eine einzelne infiltrierte Übertragungs-Unterstation führten zu Stromausfall in Kiew

2017 Petya/Not-Petya/Moonraker-Petya Nutzung von NSA-Exploits für destruktive Ransomware

2018 VPN-Filter Neustartresistente IoT-Malware für Netzwerkgeräte zur Überwachung von SCADA-Protokollen mit Bricking

Schlußbetrachtung

Die Zusammenarbeit zwischen Organisationen ist entscheidend für die Erkennung, Zuordnung und Abwehr von Cyberattacken.

Der Trend in der Cybersicherheit geht weg von der reinen Analyse von Angriffen und Schadsoftware zur aktiven Gegenspionage, sodass die führenden APTs aufgeklärt werden konnten.

Nachdem lange Zeit die Vorstellung des Cyberspace als virtueller Welt dominierte, setzt sich in Sicherheitskreisen ein immer physischeres Verständnis durch: wer die Geräte und die Leitungen kontrolliert, der kontrolliert auch die darin befindlichen Daten.

Die Furcht vor Vergeltung erklärt die große Kluft zwischen Spionageaktivitäten und echten Angriffen auf die smart industry, obwohl die technischen Möglichkeiten für weitreichende Angriffe ständig zunehmen.

Literatur

2010-2019 Online-Paper Cyberwar-Grundlagen-Methoden-Beispiele (deutsche Version)

http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-grundlagen-geschichte-methoden.pdf

2010-2019 Online-Paper Cyberwar-methods and practice (English Version)

http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf