Malware-Steckbriefe

Begleitmaterial zum City Lab Workshop IT-Sicherheit

City Lab Südwestfalen

Computervirus

Name	Virus
Namensgeber	Aus der Biologie: wie auch ein „echter“ Virus benötigt ein Computervirus einen Wirt (ausführbare Programme), um „überleben“ zu können
Infektion	• E-Mail: Versand ausführbarer Dateien oder Hyperlinks • Wechseldatenträger: Bei Übertragung infizierter, ausführbarer Dateien
Ziel	Datenraub oder Löschen von Daten
Undercover?	Ja
Verbreitung	Innerhalb eines Computers: Der Virus kopiert sich selbst an eine noch nicht infizierte Datei
Auswirkung	Verlust von Daten
Bedrohte Schutzziele	Integrität
Gegenmaßnahmen	Nutzung von Anti-Viren Software

City Lab Südwestfalen

Computerwurm

Name	**Wurm / Würmer**
Namensgeber	Würmer schlüpfen durch ein (Sicherheits-)Loch und benötigen im Vergleich zum Virus keinen Wirt sondern können unabhängig „überleben“
Infektion	• E-Mail: Versand ausführbarer Dateien oder Hyperlinks • Instant-Messaging: Linkversand über Messenger, dessen Website den Wurm enthält • Wechseldatenträger: Würmer kopieren sich selbst auf einen USB-Stick und verbreiten sich so auf anderen Computern • Bluetooth: Bei Smartphones und anderen mobilen Endgeräten
Ziel	Datenraub oder Löschen von Daten
Undercover?	Ja
Verbreitung	Vervielfältigen sich rasch über Netzwerke und Bluetooth-Schnittstellen
Auswirkung	Erzeugen einer hohen Systemlast und Überlastung des Netzwerks → Ausfall von Servern
Bedrohte Schutzziele	Vertraulichkeit, Verfügbarkeit
Gegenmaßnahmen	Schutz vor Social Engineering | Anti-Viren Software | Firewall

City Lab Südwestfalen

Trojaner

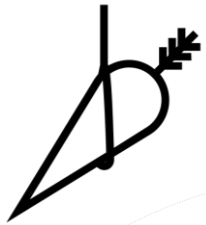
Name	**Trojanisches Pferd (umgangssprachlich „Trojaner“)**
Namensgeber	Die griechische Sage von Troja und dem trojanischen Pferd
Infektion	Download / Installation eines vermeintlich nützlichen Programmes
Ziel	• Ermöglichen Zugänge für den Angreifer, um auf das befallene System zugreifen zu können • Sammeln von geheimen Informationen (z. B. Passwörter oder Kreditkartendaten)
Undercover?	Nein
Verbreitung	Vervielfältigen sich rasch über Netzwerke

Auswirkung	• Abhängig von dem Zweck des Trojaners, z. B.:
	  • Remote-Steuerung durch den Angreifer (Backdoor)
	  • Verschlüsselung des Computers (Ransomware)

Bedrohte Schutzziele	Vertraulichkeit | Verfügbarkeit | Integrität
Gegenmaßnahmen	Schutz vor Social Engineering → „Halten Sie die Tore geschlossen“ | Anti-Viren Software

City Lab Südwestfalen

Social Engineering



Name	**Social Engineering (der Mensch als Schwachstelle)**
Namensgeber	Der „Faktor Mensch“ wird als vermeintlich schwächstes Glied in der Sicherheitskette ausgenutzt
Infektion	E-Mail (s. Phishing) oder soziale Medien – Der Angreifer täuscht das Opfer mit einer vertrauenswürdigen Identität und manipuliert dieses dadurch
Ziel	• Einschleusen von Schadsoftware • Abgreifen von vertraulichen Daten
Undercover?	Ja / Nein – einem aufmerksamen Opfer kann der Täuschungsversuch auffallen
Verbreitung	Abhängig vom Ziel / Schadprogramm
Auswirkung	Häufig wird von den Opfern Geld verlangt indem beispielsweise eine Ransomware (Erpressungstrojaner) oder eine Scareware (Schadprogramm, die das Opfer verängstigt, um eine gewünschte Reaktion hervorzurufen) installiert wird
Bedrohte Schutzziele	Vertraulichkeit | Verfügbarkeit
Gegenmaßnahmen	Verantwortungsvoller Umgang mit sozialen Medien und E-Mails von fragwürdigen Absendern | Sensibilisierung und Schulung von Mitarbeitern

City Lab Südwestfalen

Brute-Force Angriff

Name	**Brute-Force**
Namensgeber	Nutzt „rohe Gewalt“ (brute force)
Infektion	Nutzung bekannter E-Mail Adressen und Nutzernamen
Ziel	Erraten von Passwörtern, um Zugang zu Online-Konten zu erhalten
Undercover?	Ja
Verbreitung	Wenn Passwörter mehrfach verwendet werden kann ein Zugang zu verschiedenen Konten erfolgen
Auswirkung	• Aussperren des Nutzers • Tätigen von Transaktionen (Banking, Shopping) • Änderung von Daten und Design auf Webseiten
Bedrohte Schutzziele	Vertraulichkeit
Gegenmaßnahmen	Passwortmanagement, Login-Schutz

City Lab Südwestfalen

Distributed-Denial-of-Service (dDoS)

Name	**dDoS (distributed-Denial-of-Service)**
Namensgeber	Denial of Service bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der normalerweise verfügbar sein sollte
Infektion	Nutzung von Botnetzen aus infizierten Rechnern
Ziel	• Überlastung eines Internetdienstes, um diesen unbrauchbar für Nutzer zu machen
Undercover?	Nein
Verbreitung	Ein einfacher DoS Angriff erfolgt von einem Host, wohingegen ein dDoS Angriff über ein gesamtes Botnetzwerk stattfindet: im Vorfeld wurden bereits mehrere Rechner in einem Netzwerk durch die Verbreitung von Backdoor Trojanern infiziert, die zu einem Botnetz verbunden werden
Auswirkung	• Umsatzeinbußen durch Ausfall des Online-Shops • Reputationsverlust bei den Kunden • Wirtschaftliche Schäden für das betroffene Unternehmen
Bedrohte Schutzziele	Verfügbarkeit
Gegenmaßnahmen	Anti-Viren Software zur Abwehr von Backdoor-Angriffen | Firewall (für einfache dDoS Angriffe) | Spezielle Software für den Schutz gegen dDoS Angriffe

City Lab Südwestfalen

Ransomware

Name	**Ransomware oder auch Erpressungstrojaner**
Namensgeber	Ransom steht im Englischen für „Lösegeld“ oder „Freikauf“, da von dem Opfer Lösegeld verlangt wird
Infektion	• Clouddienste • E-Mail Anhänge • Sicherheitslücken im Web-Browser
Ziel	• Verschlüsseln des Computers, damit das Opfer nicht mehr auf seine Daten zugreifen kann • Verlangen von Lösegeld, um den „Schlüssel“ von dem Angreifer zu erhalten
Undercover?	Nein
Verbreitung	Einmal infiziert, kann eine Ransomware ein gesamtes Netzwerk befallen
Auswirkung	Verschlüsselung des Computers von dem Angreifer
Bedrohte Schutzziele	Vertraulichkeit | Verfügbarkeit
Gegenmaßnahmen	Regelmäßige Back-Ups | Virenschutz | Nutzung einer Firewall

City Lab Südwestfalen

Phishing

Name	**Phishing**
Namensgeber	Setzt sich aus den englischen Worten „Password“ und „Fishing“ zusammen
Infektion	• Öffnen von Hyperlinks in einer Phishing Mail • Folgen von Links vermeintlicher Werbung in den sozialen Medien
Ziel	• Abfangen von Anmeldedaten (Benutzernamen und Passwörter) • Datendiebstahl • Angriff auf kritische Infrastrukturen • Installation von Schadsoftware
Undercover?	Ja / Nein – einem aufmerksamen Opfer kann der Täuschungsversuch auffallen
Verbreitung	Abhängig von dem Schadprogramm
Auswirkung	Meistens werden Passwörter abgefangen die bei dem Opfer einen finanziellen Schaden, durch den Missbrauch eines Kontos, verursachen
Bedrohte Schutzziele	Vertraulichkeit
Gegenmaßnahmen	Spam-Ordner für das E-Mail Postfach | Schulung & Sensibilisierung der Mitarbeiter | Firewall

City Lab Südwestfalen

Mail-Spoofing

Name	Spoofing
Namensgeber	To spoof = manipulieren, vortäuschen, verschleiern
Infektion	Zufall (erratene Emailadresse), Daten-Leak
Ziel	Versand von Spam im falschen Namen zur Verbreitung von Schadprogrammen (Downloads) oder Datenklau (Phishing)
Undercover?	Nein
Verbreitung	Spam kann von der eigenen Adresse an die eigenen Kontakte versendet werden. Besonders kritisch bei geschäftlichen Mail-Adressen
Auswirkung	Falschinformation, Vertrauensverlust in die Absender-Adresse. Ansonsten nichts, solange die E-Mails ignoriert werden
Bedrohte Schutzziele	Klassische Ziele nur indirekt bedroht; direkt bedroht: Authentizität
Gegenmaßnahmen	E-Mail ignorieren, eigene Kontakte warnen, Mail-Provider kontaktieren

City Lab Südwestfalen

Quellenangaben

- Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi-fuer-buerger.de/
- Eckert (2018): IT-Sicherheit – Konzepte, Verfahren, Protokolle
- Hellmann (2018): IT-Sicherheit - Eine Einführung
- Weber, Gabriel, Lux, Schroer (2019): Basiswissen Wirtschaftsinformatik