Università della Svizzera italiana

High Noon im Cyberraum

Bedrohungen der Cybersicherheit für Unternehmen und Verwaltung

Prof. Dr. Marc Langheinrich
Università della Svizzera Italiana (USI)

1

1

Firma kontrolliert nach eigenen Angaben 40% der US-Getreideproduktion und Futter für über 11 Millionen Tiere

chicken1

10 von 120 Mitarbeitern von „NEW Cooperative“, Iowa hatten „chicken1“ als Passwort. Firma war im September 2021 Ziel eines Ransomware-Angriffs. Angreifern forderten 5,9 Millionen US-Dollar Lösegeld – es ist nicht bekannt, ob Firma diese Summe zahlte.

Insgesamt waren bei „NEW Cooperative“ über 650 Konten kompromittiert!

2

2

Università della Svizzera italiana

Ransomware!

- 66% von über 3'000 befragten Unternehmen waren im letzten Jahr von Ransomware-Angriffen betroffen. (Sophos, 2023)
- Schätzungen gehen von weltweit 10-20 Ransomware-Angriffen pro Sekunde aus – mindestens 10 pro Tag sind erfolgreich. (AAG, 2023)
- 2021 zahlte eine Versicherungsgesellschaft Lösegeld von 40 Millionen US-Dollar – Weltrekord! (Business Insider, 2021)
- Die durchschnittliche Ausfallzeit, die ein Unternehmen nach einem Ransomware-Angriff erleidet, beträgt 21 Tage. (Coveware, 2021)

3

3

6

Università della Svizzera italiana

Die Burg als Sicherheitskonzept

7

Bildquelle: TES

7

Università della Svizzera italiana

Cybersicherheitskomponenten

Netzsicherheit

Servers

Databases

API Security

- Application Security
- Security Engineering
- Vulnerability Testing
- Penentration Testing
- Network Intrusion Detection Systems
- Firewalls

Internet Security

- HTTPS
- SSL Certificates
- OAuth 2.0

Cloud Security

- OAuth 2.0
- Web Sockets

Endgerätesicherheit

Computer Security

Mobile Security

Users

- Email Security
- VPNs
- Encryption
- Anti-Malware

Wireless Security

Angriffspunkte

Und

Sicherheitsmechanism

Quelle: Exabeam

8

Bildquellen: [1] 850 Medieval Wonders (pinterest.se) und [2] Doves and Pigeons in History (Wysinfo)

8

Università della Svizzera italiana

Prinzip des schwächsten Glieds

- Burgmauer („Firewall“) ist oft nur schwer zu überwinden
- Tresor („Kryptographie“) ist praktisch unaufbrechbar
- Angreifer müssen einfachere Wege finden
  - Einschleichen, wenn sich Tor für autorisierte Besucher öffnet
  - Stehlen, wenn der Tresorraum zwecks Einlagerung offen steht
  - Wachen ablenken und Schlüssel aus der Tasche ziehen

9

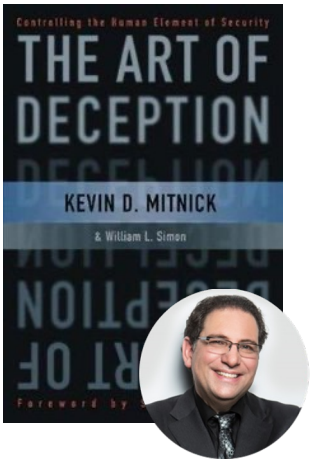
Bildquelle: William Kilmer auf LinkedIn

9

Università della Svizzera italiana

„Social Engineering“

- Grundprinzip: User austricksen, nicht Code
- Erfolgreichste Methode des Hackings
  - bekannt geworden durch Kevin Mitnick (‘88, ‘95)
  - „die psychologische Manipulation von Menschen, um Handlungen auszuführen oder vertrauliche Informationen preiszugeben“ (Wikipedia)
- Wird bei 98 % der Cyberangriffe verwendet [purplesec.us]
- Zentrales Werkzeug: „Phishing“



10

10

Università della Svizzera italiana

Phishing

- Senden einer betrügerischen E-Mail, die den Empfänger dazu verleitet
  - einen Link zu klicken und Anmelde-daten auf falscher Website einzugeben
  - ein infiziertes Dokument zu öffnen
  - Schadsoftware auszuführen
- Häufigste Cyberangriffsart!
  - Mehr als zwei Drittel aller Angriffe [Quelle: FBI]
  - Über 10% der Empfänger klicken schädlichen Link [purplesec.us]


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Bildquelle: Wikipedia

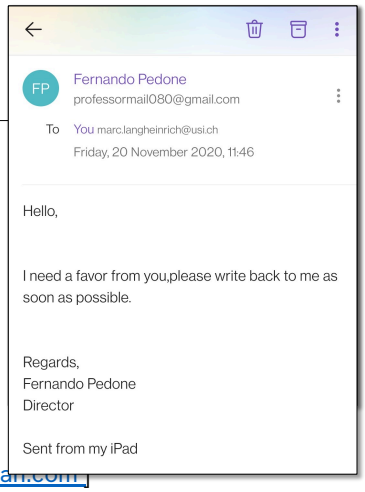
11

11

Università della Svizzera italiana

„Speerfischen“ (Spear Fishing)

- Gezielte E-Mails unter Ausnutzung bestehender Beziehungen
  - Basiert beispielsweise auf öffentlichen Websites & Facebook-Streams, oder E-Mails, die in einem gehackten Konto gefunden wurden
- Erhöht die Wahrscheinlichkeit einer Antwort
  - Mobile Bildschirme machen dies noch einfacher (siehe Beispiel), da E-Mail-Adressen häufig abgekürzt oder ausgeblendet werden
  - 2/3 aller Phishingangriffe sind Spearphishing [tessian.com]
- Eine **Übernahme des E-Mail- bzw. Social-Media-Kontos** des Opfers macht es nahezu unmöglich, Betrug zu erkennen!


FP Fernando Pedone
professormail080@gmail.com
To You marc.langheinrich@usi.ch
Friday, 20 November 2020, 11:46

Hello,

I need a favor from you,please write back to me as soon as possible.

Regards,
Fernando Pedone
Director

Sent from my iPad

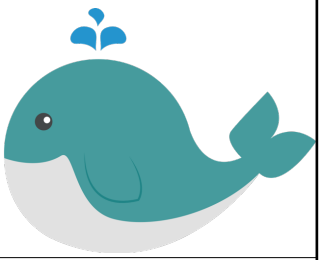
12

12

Università della Svizzera italiana

„Walfang“ (Whaling)

- Spear-Phishing, welches auf hochrangige Ziele abzielt (z.B. leitende Angestellte)
  - Gut formulierte E-Mail mit aufschreckendem Thema (z.B. gerichtliche Vorladung)
  - Viele verwertbare Informationen verfügbar (z.B. LinkedIn)
- Auch umgekehrt möglich („CEO Fraud“)
  - Angeblich vom CEO gesendete E-Mails
  - Bei gezielter Umsetzung kann dies beispielsweise umfangreiche Überweisungen auf Offshore-Konten auslösen



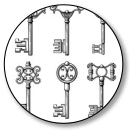
13

13

Università della Svizzera italiana

Phishing-Resultate

1. Kontoanmeldeinformationen
   - „Schlüssel zum Schloss“ (oder von einigen Gebäuden)



2. Installation schädlicher Software
   - „Kriminelle in der Palastwache“ (oder der Küche…)

- Dann: „Eskalation“ von Berechtigungen
  - „Beförderung vom Laufburschen zum Burgverwalter“
  - Der Angreifer versucht dabei, so lange wie möglich unentdeckt zu bleiben

14

Bildquellen: Vintage mittelalterliche Schlüssel, antike Chaves lizenzfreie Vektoren , Leben in einem Schloss – Enzyklopädie der britischen Geschichte für Kinder und Das Haushaltspersonal in einem englischen mittelalterlichen Schloss – Enzyklopädie der Weltgeschichte

14

Università della Svizzera italiana

Andere Wege „ins Schloss“

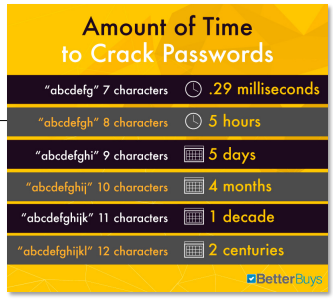
1. Konto-Hacking (d.h. nicht auf Phishing-Basis)
   - Sowohl Firmenkonten als auch Privatkonten bergen Risiken
2. Anfällige, nach außen gerichtete Software
   - z.B. Remote-Desktop-Software (RDP)
3. Zero-Day-Exploits
   - Kaseya-Angriff (2021) durch REvil betrifft 1000+ Unternehmen
4. Angriff auf die Software-Lieferkette („Supply Chain“)
   - SolarWinds (2020) kompromittierte White House-Systeme

15

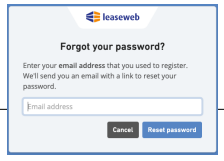
15

Università della Svizzera italiana

1. Account-Hacking



- Kurze Passwörter!
  - Bis zu 10 Zeichen können auf PC geknackt werden
  - Datenbasis: “geschützte” (hashed) Anmelde-DB
- Wiederverwendung von Anmeldedaten
  - Viele Nutzer verwenden dasselbe (schwache) Passwort
    - „chicken1“, „123456“, „password“
  - Viele Nutzer verwenden für verschiedene Dienste dasselbe Passwort
  - Finden des Passworts für einen Dienst/Benutzer hilft, andere zu finden
- E-Mail-Konto oft entscheidend für den Zugriff auf andere Konten!
  - Bei den Funktionen zum Zurücksetzen des Passworts wird davon ausgegangen, dass der Benutzer die Kontrolle über E-Mails hat
- Gehackte Accounts (auch private) können als Plattform für Spear-Phishing-Angriffe dienen!



16

16

Università della Svizzera italiana

2. Anfällige Software (Netzwerkbereich)

- Remote Desktop-Protokoll (RDP)
  - Desktop-Zugriff für Endbenutzer und IT Support
- VPN (Virtuelles privates Netzwerk)
  - Mitarbeitern Zugriff auf Unternehmensressourcen gewähren
- „IT-Management"-Dienste (z.B. SSH, rsync)
  - Unterstützen Hintergrunddienste, z. B. für Dateisynchronisierung und Backup
- APIs („Application Programming Interface")
  - Programmierschnittstelle für webbasierte Anwendungen (dynamische Daten)

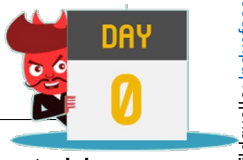
Alle oben aufgeführten Dienste können sowohl „gehackt" werden (d. h. bekannte Fehler können zum „Anmelden" genutzt werden) als auch mit gestohlenen Benutzerdaten genutzt werden

17

17

Università della Svizzera italiana

3. Zero-Day-Schwachstellen



Bildquelle: Indusface

- Ursprünglich: Software, die direkt vom Entwickler gestohlen wurde („0 Tage seit Veröffentlichung")
- Heute: **Schwachstellen**, die bisher **unbekannt** waren (der Entwickler kennt sie möglicherweise schon, oder auch nicht).
  - **Bekannte** Schwachstellen (also nicht 0-Day) sind immer noch sehr gefährlich, da Updates Zeit brauchen oder Kunden sie nicht einspielen!
- Unbekannte Schwachstellen werden auf dem illegalen Hackermarkt hoch geschätzt, da es keine bekannten Abhilfemaßnahmen („Patches") gibt
  - Unbekannte Schwachstellen haben sehr hohe Erfolgsaussichten!
- Werden auch häufig von Geheimdiensten verwendet

18

18

Università della Svizzera italiana

4. Software Lieferketten-Angriffe

- Software benötigt zunehmend „Lieferketten“ (wie Autos)
  - verwendet vorgefertigte **Bauteile** (Bibliotheken), sowohl kommerzielle als auch Open-Source
  - nutzt **Tools** von Drittanbietern (z. B. Editoren, Codeverwaltung)
  - nutzt ausgefeilte **Distributions-infrastruktur** für Updates

Bildquelle: Dribble

- Angreifer „schmuggeln“ Schadcode und Funktionalität irgendwo „Upstream“ ein
  - Der Kunde erhält ein scheinbar gültiges, unverfälschtes Programm von einem vertrauenswürdigen, seriösen Anbieter!

19

19

20

Università della Svizzera italiana

Angriffsausnutzung

- Geld stehlen
  - Beispiel: CEO-Betrug, um Überweisung auf Offshore-Konto zu erwirken
  - Privater Kontext: Leute dazu bringen, über Western Union zu bezahlen
- Geheimnisse stehlen
  - Erpressung zwecks Nichtoffenlegung von Unternehmensdaten
  - Privater Kontext: Drohung, private Bilder preiszugeben
- Daten-„Entführung“ (Ransomware-Angriff)
  - Daten verschlüsseln und Zahlung gegen Schlüssel verlangen
- Als Angriffsplattform etablieren
  - Dauerhaft unbemerkten Zugriff einrichten (z.B. für Betrieb Botnet)

Oft kombiniert

21

21

Università della Svizzera italiana

Beispiel WannaCry (Mai 2017)

- Ursprung wohl in Nord-Korea
- Nutzt Zero-Day Exploit in Windows
  - Angeblich bereits in 2011 von der NSA entwickeltes Tool (EternalBlue)
  - In 2016 Diebstahl durch Hacker, daher Meldung durch NSA an Microsoft
- Microsoft-Patch im April 2017
  - Nur wenige Unternehmen hatten Systeme aktualisiert
  - 300’000 infizierte Rechner in 8h (12.5.)
- Glücklicherweise schlecht programmiert
  - Sicherheitsexperte findet “kill switch” und stoppt weitere Verbreitung

23

23

Università della Svizzera italiana

Warum ist Ransomware so „beliebt“?

- Unternehmensdaten sind sehr, sehr wertvolle Ressource!
  - Unternehmen können ohne Zugriff auf ihre Daten nicht agieren
  - „Grosswildjagd“ statt individuelle PCs von Endnutzern verschlüsseln

24

24

Università della Svizzera italiana

Angriffsbeispiele “Grosswild”

- Dezember 2020: SolarWinds (US-Regierung, Microsoft, …)
  - Lieferkettenangriff auf Netzwerktool im Frühjahr 2020, womöglich aber schon viel früher (2017)
  - Geschätzte 18’000 Kunden betroffen, hauptsächlich in USA
- Mai 2021: Colonial Pipeline
  - betreibt grösste Pipeline zwischen Texas und US-Ostküste (45%)
  - Abrechnungssystem betroffen, kein Verkauf für 6 Tage möglich
  - Firma zahlte $4.4 Millionen Lösegeld
- Juni 2023: MoveIT (British Airway, BBC, Boots, …)
  - Zero-Day-Schwachstelle in weit verbreitetem Dateitransfer-Tool
  - Hacker drohen mit Datenveröffentlichung

25

25

Università della Svizzera italiana

Warum ist Ransomware so „beliebt“?

- Unternehmensdaten sind sehr, sehr wertvolle Ressource!
  - Unternehmen können ohne Zugriff auf ihre Daten nicht agieren
  - „Grosswildjagd“ statt individuelle PCs von Endnutzern verschlüsseln
- Aufstieg von „RaaS“: Ransomware-as-a-Service
  - Hackergruppen bieten Ransomware-Angriffe gegen Pauschalgebühr plus Teil des erpressten Betrags an (z. B. „Netwalker“).
  - Gruppen stellen die gesamte Infrastruktur bereit – außer Grundgebühr keine Investitionen seitens des „Kunden“ erforderlich
  - Partnerprogramm: Andere Gruppen stellen (gekaperte) Computer oder Websites zur Verfügung, um Angriffe durchzuführen.

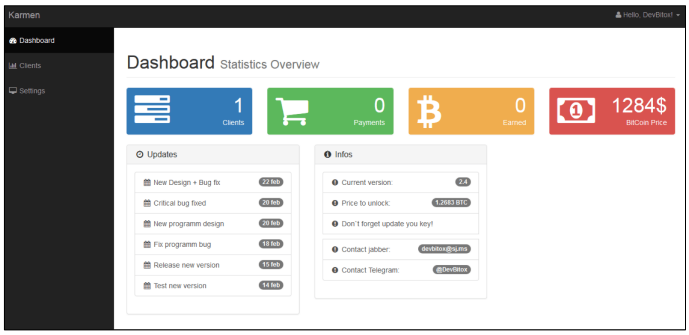
26

26

Università della Svizzera italiana

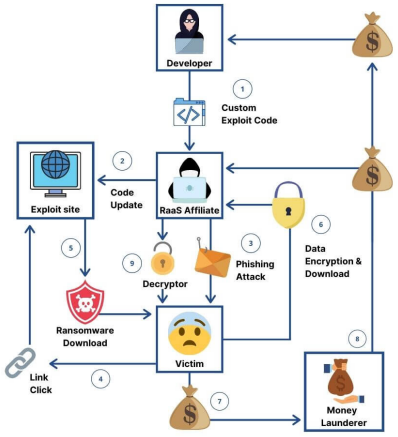
Ransomeware-as-a-Service

RaaS-Client-Dashboard



Bildquelle: Threatpost.com

RaaS-Partnerprozess



Bildquelle: UpGuard

27

27

Università della Svizzera italiana

Warum ist Ransomware so „beliebt“?

- Unternehmensdaten sind sehr, sehr wertvolle Ressource!
  - Unternehmen können ohne Zugriff auf ihre Daten nicht agieren
  - „Grosswildjagd“ statt individuelle PCs von Endnutzern verschlüsseln
- Aufstieg von „RaaS“: Ransomware-as-a-Service
  - Hackergruppen bieten Ransomware-Angriffe gegen Pauschalgebühr plus Teil des erpressten Betrags an (z. B. „Netwalker“).
  - Gruppen stellen die gesamte Infrastruktur bereit – außer Grundgebühr keine Investitionen seitens des „Kunden“ erforderlich
  - Partnerprogramm: Andere Gruppen stellen (gekaperte) Computer oder Websites zur Verfügung, um Angriffe durchzuführen.
- Sehr „benutzerfreundlicher“ Zahlungsvorgang ☺
  - Detaillierte Anleitung zum Bezahlen mit Kryptowährung!
- Zusatzverdienst: Androhung der Veröffentlichung der Daten

28

28

29

Università della Svizzera italiana

Herausforderungen

- Essenziell: Schulung der Mitarbeiter auf allen Ebenen
  - Phishing funktioniert!
- Komplexität IT-Landschaft I: Mitarbeiter
  - Von „BYOD“ bis Home Office
  - Persönliche Geräte oft weniger sicher
- Komplexität IT-Landschaft II: Systeme
  - Angriffsfläche („attack surface“) wächst stetig
  - Es kann jeden treffen: Schulen, Unis, KMUs, Not-for-Profit, …

30

30

Università della Svizzera italiana

Vier Ansätze für Cyber-Sicherheit

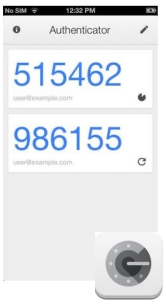
1. Schutz
   - Mechanismen die **überwunden** werden müssen
     - z.B. Passwort
2. Abschreckung
   - **Konsequenzen** wenn der Angriff fehlschlägt
     - z.B. Gesetze
3. Widerstandsfähigkeit
   - **Folgen** erfolgreicher Angriffe **minimieren**
     - z.B. Backups
4. Erkennung und Wiederherstellung
   - Angriff erkennen und **Gegenmaßnahmen** einleiten
     - z.B. System runter fahren

31

31

Università della Svizzera italiana

Authentisierung: Ende der Passwörter



- Verpflichtende Passwort-Updates unsicher!
  - Balance zwischen Sicherheit und Produktivität finden
- Von Passwörtern zu Multi-Faktor-Authentifizierung
  - Zweitfaktor- und Multifaktor-Authentisierung (2FA, MFA)
- Passkeys – Kryptographische, gerätegebundene Tokens
  - Werden z.B. auf Telefon sicher hinterlegt und biometrisch entsperrt
  - Phishing? Verifizierung erfolgt auf Gerät selbst (kein PW an Webseite)
  - Passwortdatenbank-Diebstahl? Physisches Gerät wird benötigt!

32

32

Università della Svizzera italiana

Vorbereitung ist alles!

- Bereiten Sie sich auf Ransomware-Angriffe vor
  - Offline-Backups (erfordert Früherkennung)
  - Halten Sie für den Fall eines Falles ein „Notfallskript“ bereit
- Neue Risiken durch ChatGPT?!
  - Spear-Phishing, Whaling immer schwerer zu durchschauen!
  - Beschleunigte (einfacherere) Entwicklung von Schadsoftware!
- Aber auch: Hilfe durch KI/ChatGPT
  - Dialogbasierte, kontextsensitive Assistenzsysteme für Ernstfall
  - Verbesserte Unterscheidung legitime/illegitime Aktivitäten
  - Unterstützung bei sicherer Softwareentwicklung

33

33

Università della Svizzera italiana

Herzlichen Dank für Ihre Aufmerksamkeit

4 Ansätze für Sicherheitsdienste

1. Schutz
   - Mechanismen die über-wunden werden müssen
     - z.B. Verschlüsselung
2. Abschreckung
   - Konsequenzen wenn der Angriff fehlschlägt
     - z.B. Gesetze
3. Widerstandsfähigkeit
   - Folgen erfolgreicher Angriffe minimieren
     - z.B. Backups
4. Erkennung und Wiederherstellung
   - Angriff erkennen und Gegenmaßnahmen einleiten
     - z.B. System runter fahren

Die Burg als Sicherheitskonzept

Warum ist Ransomware so „beliebt“?

- Unternehmensdaten sind sehr, sehr wertvolle Ressource!
  - Unternehmen können ohne Zugriff auf ihre Daten nicht agieren
  - „Grosswildjagd“ statt individuelle PCs von Endnutzern verschlüsseln
- Aufstieg von „RaaS“: Ransomware-as-a-Service
  - Hackergruppen bieten Ransomware-Angriffe gegen Pauschalgebühr plus Teil des erpressten Betrags an (z. B. „Netwalker“).
  - Gruppen stellen die gesamte Infrastruktur bereit – außer Grundgebühr keine Investitionen seitens des „Kunden“ erforderlich
  - Partnerprogramm: Andere Gruppen stellen (gekaperte) Computer oder Websites zur Verfügung, um Angriffe durchzuführen.
- Sehr „benutzerfreundlicher“ Zahlungsvorgang ☺
  - Detaillierte Anleitung zum Bezahlen mit Kryptowährung!
- Zusatzverdienst: Androhung der Veröffentlichung der Daten

28

Herausforderungen

- Essenziell: Schulung der Mitarbeiter auf allen Ebenen
  - Phishing funktioniert!
- Komplexität IT-Landschaft I: Mitarbeiter
  - Von „BYOD“ bis Home Office
  - Persönliche Geräte oft weniger sicher
- Komplexität IT-Landschaft II: Systeme
  - Angriffsfläche („attack surface“) wächst stetig
  - Es kann jeden treffen: Schulen, Unis, KMUs, Not-for-Profit, ...

30

34

34