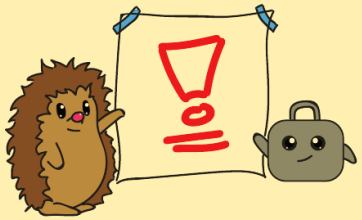
Technische Universität Braunschweig

Gauß-IT-Zentrum

Emotet – eine neue Dimension des Phishings

Dr. Christian Böttger, 28.10.2020



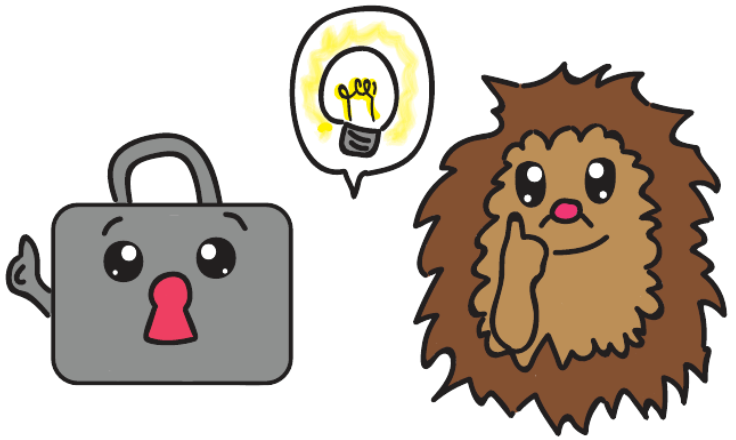
Haben sie schon einmal von Emotet gehört?

A. **Ja**

B. **Nein**

Agenda

- Phishing (ganz kurz)
- Emotet – was ist das?
- Dynamite Phishing mit Emotet
- Beispiel: Emotet bei Heise
  - Ablauf
  - Infektion
  - Gegenmaßnahmen
- Lessons learned
  - Wie verhindert man solche Angriffe
  - Wie bereitet man sich vor



Phishing

- Betrugsversuch per E-Mail oder Messenger
- Nachricht wirkt seriös, greift vielleicht sogar wirklich bestehende Konversationen auf
- Links führen zu unseriösen Websites
- Bösartige Anhänge
  - einer davon: Emotet

Bild: 1

Phishing – weitere Informationen

- Weitere Tools und Informationen:
  - **SECUSO für den Bürger / für KMU https://secuso.aifb.kit.edu/642.php**
  - **NoPhish Video (5 Minuten) https://www.youtube.com/watch?v=XeslAkZIuwY**
  - **Privacy Friendly Apps für Android: https://secuso.aifb.kit.edu/105.php**
  - **ZAC Niedersachsen Kurzvideos**
    - Zentrale Ansprechstelle Cybercrime für die nds. Wirtschaft
      - *"Die Zentrale Ansprechstelle Cybercrime für die nds. Wirtschaft ist ein polizeilicher Berater für Firmen, Verbände und Behörden bei der Prävention von Cyberkriminalität und Ihr erster Ansprechpartner im Schadensfall."*
    - **Videos:**
      - https://zac-niedersachsen.de/video/2 (E-Mails und Links)
      - https://zac-niedersachsen.de/video/3 (Makros)

Emotet -1-

- Emotet wird als Anhang an E-Mails verschickt, nutzt veraltete Office-Formate (.doc, .xls)
  - Neueste Tendenz: verschlüsselte ZIP-Dateien mit Office-Dokumenten
- Der Schadcode nutzt keine technischen Lücken aus, sondern verlässt sich darauf, dass der Nutzer das enthaltene Word-Makro freiwillig ausführt.
- Warum sollte der Nutzer das tun?
  - Der Angreifer schaltet sich in bestehende E-Mail Gespräche ein.
  - Die Angriffsmail wird getarnt, sodass es so aussieht, als ob sie von einem Geschäftspartner oder Kollegen kommt, mit dem man tatsächlich per E-Mail Kontakt hat.
  - Zusätzlich wird auf ein wirklich bestehendes Thema Bezug genommen.

Sollten Ihre daten nicht mehr aktuell sein, ändern Sie diese ebenfalls.

1 Anlage

Dat 553912 ~.doc

----Original Message-----

Sehr geehrter Herr [redacted]

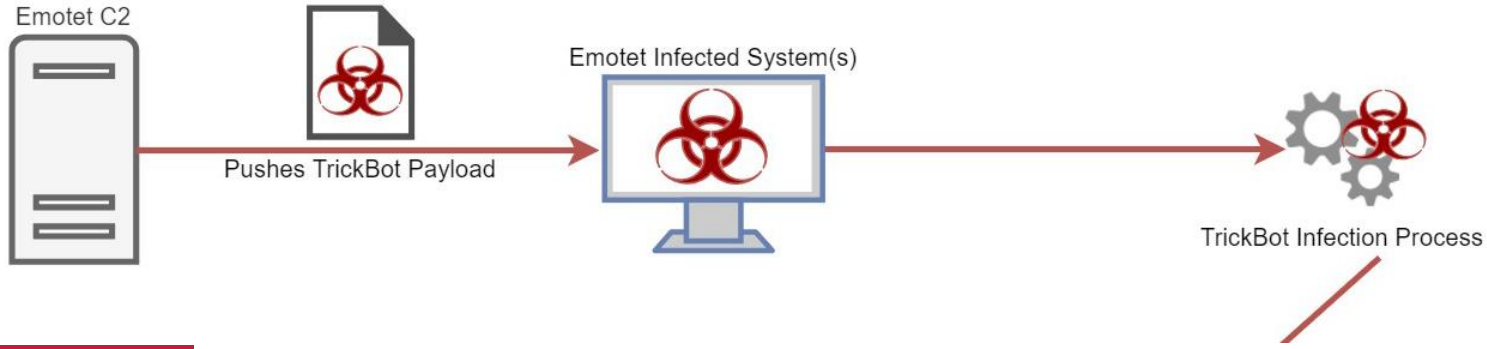
anbei erhalten Sie unterzeichnete Preisvereinbarung für 2019.

Freundliche Grüße

[redacted]

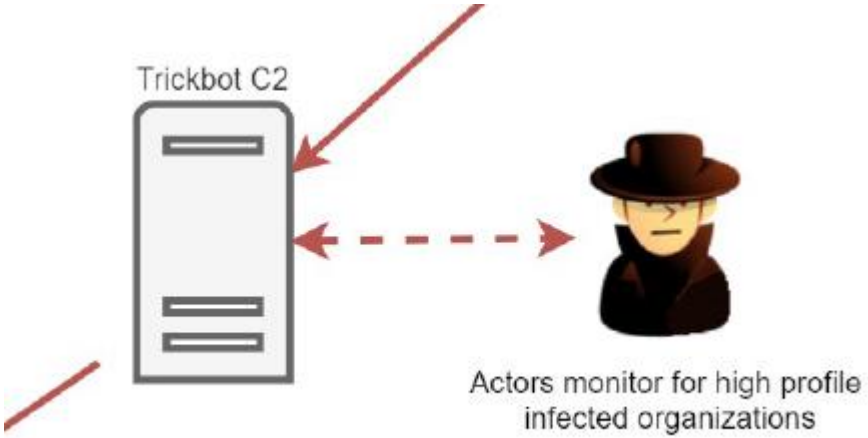
Emotet -2-

- Sobald das Makro ausgeführt wird, geht Emotet an die Arbeit:
  - 1) Das Outlook-Adressbuch des Opfers wird ausgelesen und an den „Command and Control“-Server (Abkürzungen: C&C Server, C2-Server) ausgeleitet.
  - 2) Auch das E-Mail-Postfach (mindestens die Betreffzeilen und Absender/Empfänger) werden ausgeleitet.
  - 3) Danach wird ein beliebiger, vom Angreifer festgelegter, Schadcode nachgeladen, um den eigentlichen Angriff durchzuführen
    - Weitere Infektion im Netz des Opfers,
    - Verschlüsselung, …..
    - Ausspähen, …



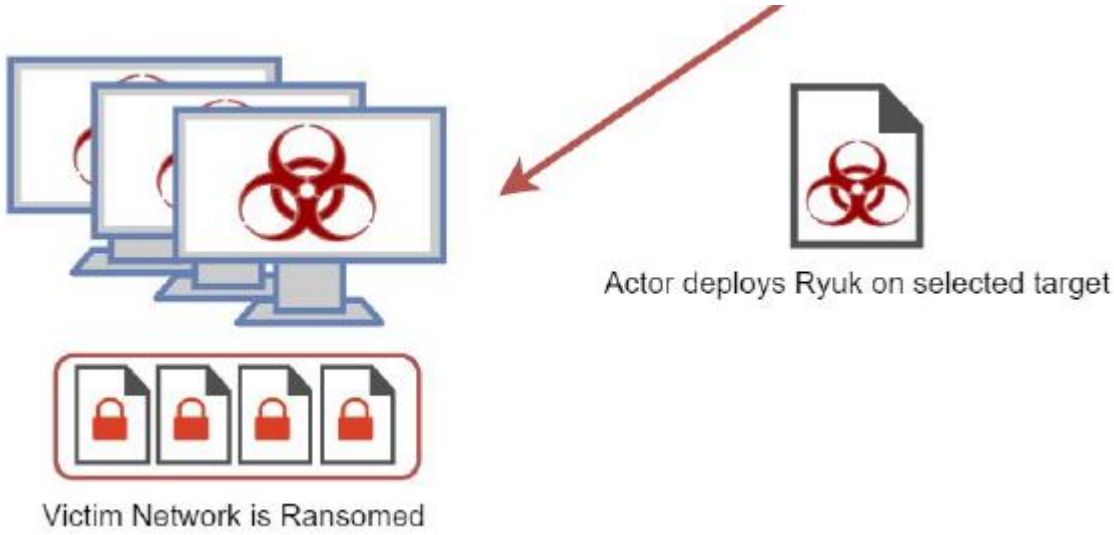
Emotet -3-

- Bis hier hin war alles automatisiert
- Im nächsten Schritt greift ein Mensch auf Angreiferseite ein: der Angreifer bewertet, aus welchen Firmen und Organisationen Meldung auf den C2-Server ankommen und sucht die Opfer heraus, die es wert sind, weiter angegriffen zu werden.

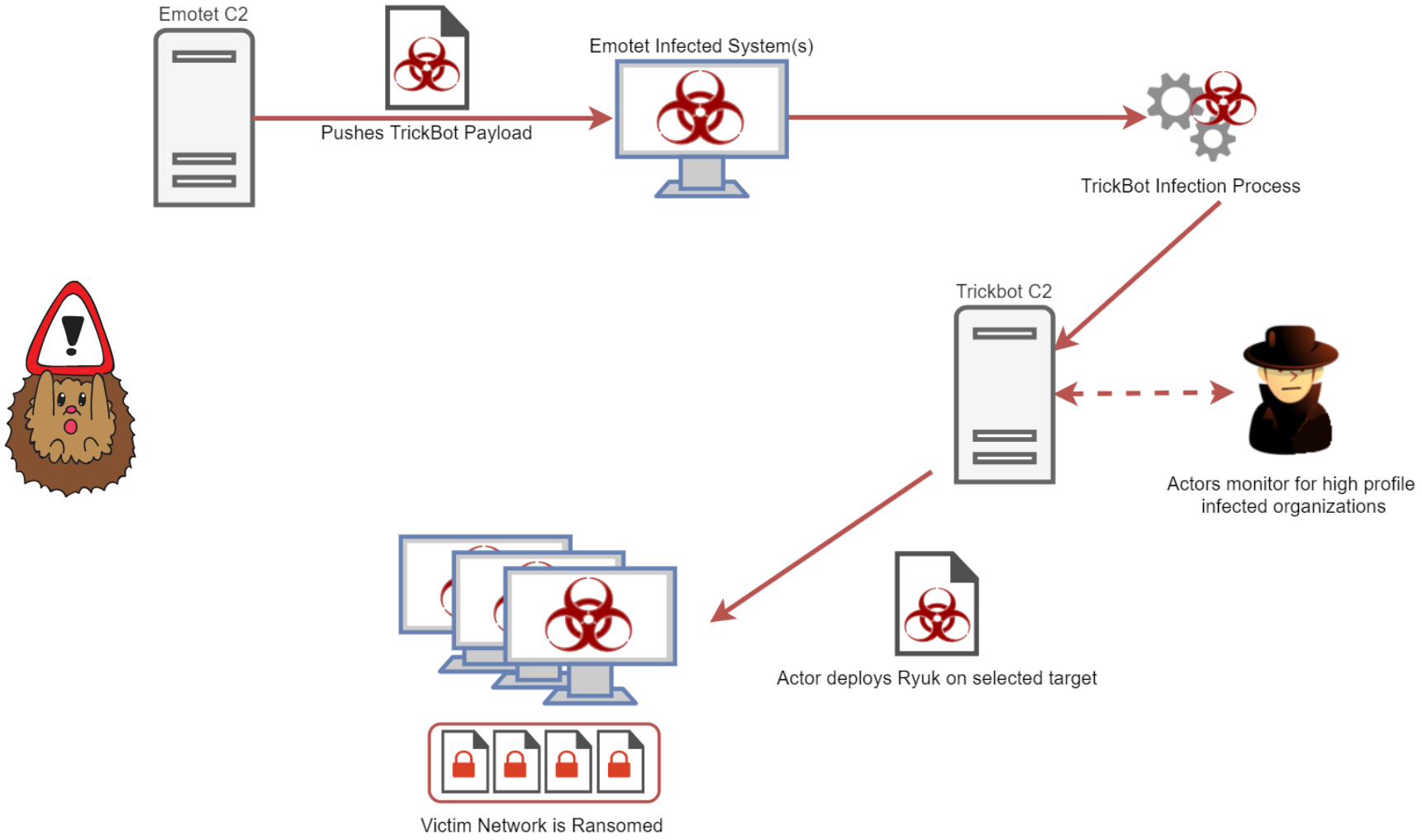


Emotet -4-

- Der Angreifer entscheidet, mit welchem Angriff es weiter geht, z.B. mit Ransomware
  - in dem Fall lässt der Angreifer z.B. die Ransomware „Ryuk“ nachladen
- In anderen Fällen vielleicht Spionage-Software oder Spam-Versand-Software
- Eventuell steuert der Angreifer auch persönlich den weiteren Angriff



Emotet -5-



https://www.kryptoslogic.com/blog/2019/01/north-korean-apt-and-recent-ryuk-ransomware-attacks/

Welche Erfahrungen haben Sie mit Schadsoftware?

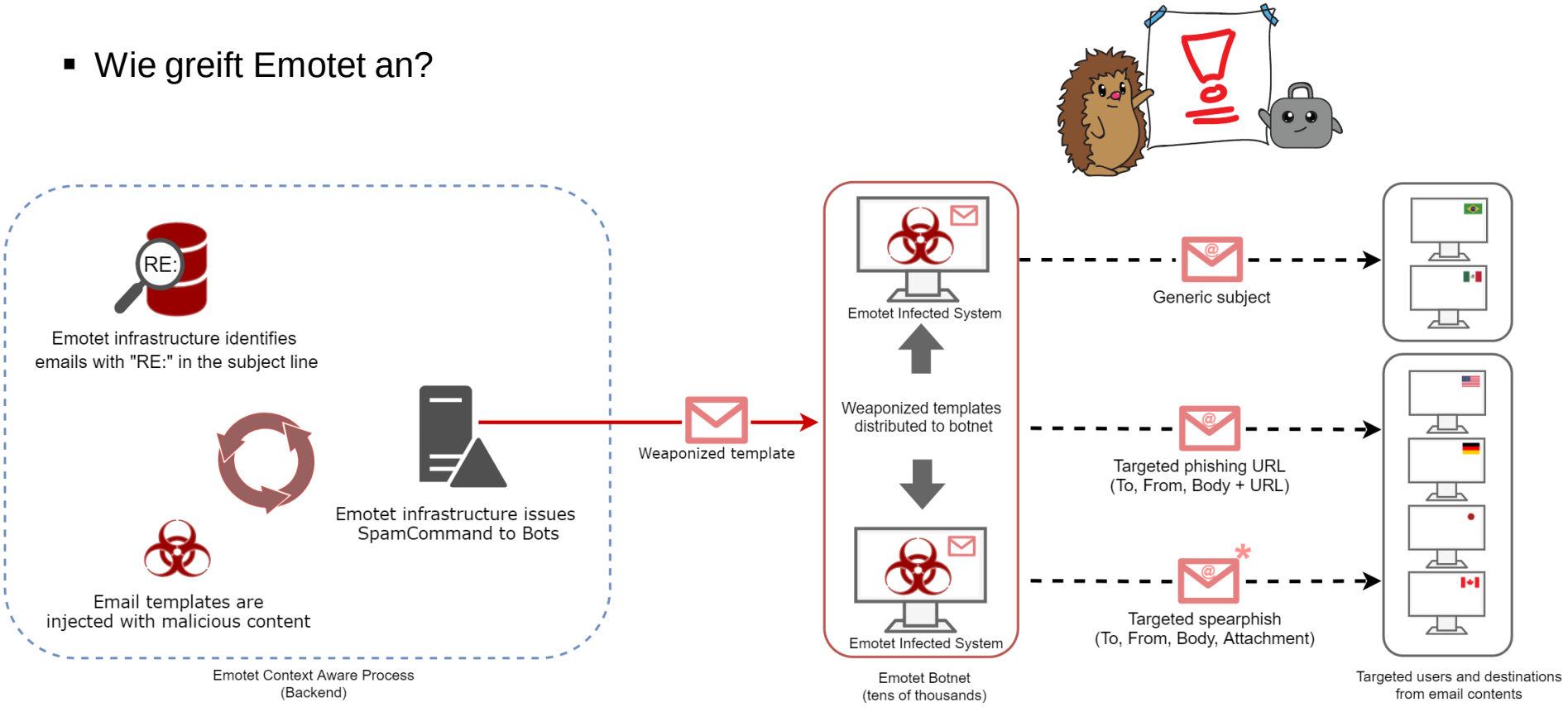
A. **Keine.**

B. **Eines meiner Geräte war mal infiziert.**

C. **Mich erreichen regelmäßig Spammails.**

Emotet – Botnet -1-

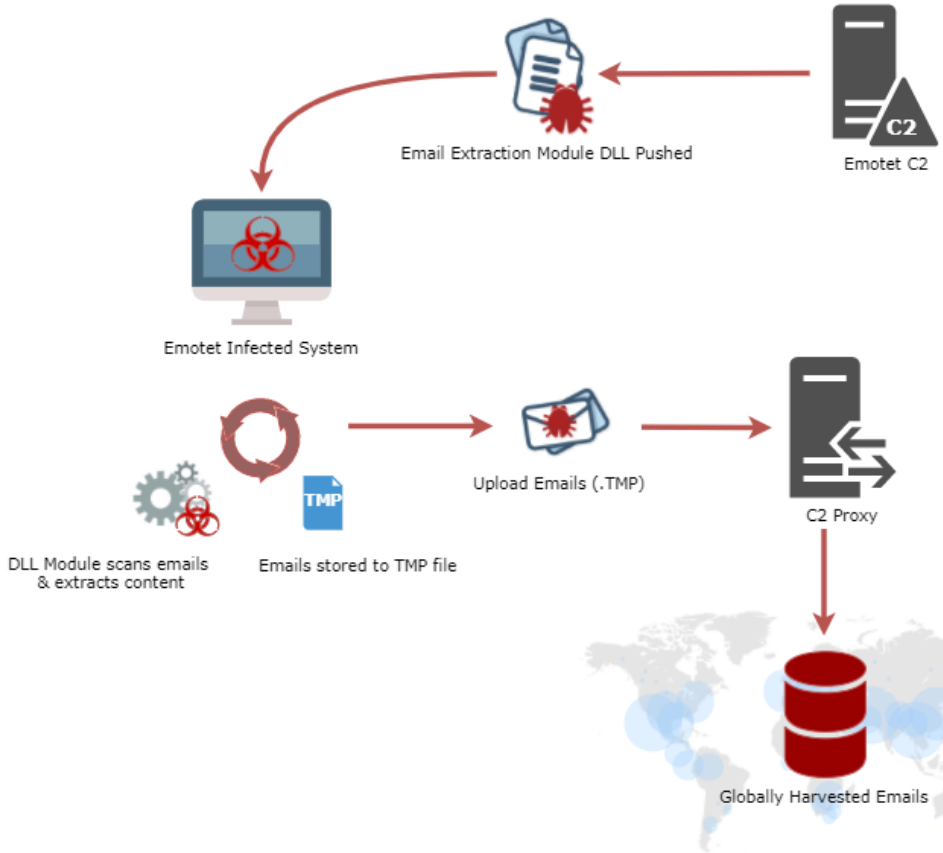
- Wie greift Emotet an?

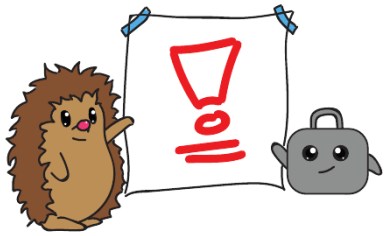


https://www.kryptoslogic.com/blog/2019/04/emotet-scales-use-of-stolen-email-content-for-context-aware-phishing/

Emotet – Botnet -2-

- Und woher kommt der verwendete Inhalt?





https://www.kryptoslogic.com/blog/2018/10/emotet-awakens-with-new-campaign-of-mass-email-exfiltration/

Emotet – verwendete Inhalte

- Welche Informationen wertet Emotet aus?
  - Nach Start eines Word/Excel-Makros:
  - Nutzung der Outlook Messaging API (MAPI) (als angemeldeter Benutzer) – kein „Hacking“
  - Auslesen aller Mails = geht alle Ordner und Unterordner im persönlichen Postfach durch
    - für jede Mail, die nicht älter als 180 Tage ist:
      - Absender Name und E-Mail
      - Empfänger Name und E-Mail
      - Betreff
      - die ersten 16384 Zeichen der Mail (16 kB)
  - Diese Informationen werden zunächst temporär auf dem Opfer-Rechner gespeichert und später zum C2-Server hoch geladen, der es in eine globale Opfer-Datenbank einpflegt.
  - Aus dieser Datenbank werden dann neue Spam-Mails mit infizierten Anhängen generiert und verschickt.

https://www.kryptoslogic.com/blog/2018/10/emotet-awakens-with-new-campaign-of-mass-email-exfiltration/

Dynamite Phishing mit Emotet

- Angreifer nutzt das bestehende ***Emotet***-Botnet
- Offenbar krimineller Konzern mit genügend Ressourcen, um die Angriffe manuell zu unterstützen
- Aus der Emotet-Mail-Datenbank werden gezielt Opfer (Firmen) heraus gesucht, von denen der Angreifer annimmt, dass sie genügend Geld flüssig haben, um eine Erpressung bezahlen zu können.

Diese Firmen werden zunächst breit gefächert mit Emotet angegriffen.

- Dabei werden real bestehende E-Mail-Kontakte aus der Emotet-Datenbank benutzt
- Sobald ein Nutzer das per E-Mail verschickte Word-Makro ausführt, wird die Schadsoftware „***Trickbot***“ nachgeladen.
- Trickbot breitet sich nun im angegriffenen Netz aus und versucht, höhere Privilegien im Active Directory des Opfers zu erbeuten.

Dabei greift ggf. auch ein Mensch auf Seiten der Angreifer mit ein.

- Sobald die angegriffene Domäne gefallen ist – also der AD Server mit Administrator-Rechten in der Hand des Angreifers ist – werden alle angeschlossenen Rechner mit der Ransom-Ware „***Ryuk***“ infiziert.
- Zum Schluss werden alle erreichbaren Datenträger verschlüsselt - und die Erpressung läuft an.

Details (technische Funktionsweise): https://heise.de/-4573848

Ablauf bei Heise

- Montag (13.5.) ca 15:00: Erstinfektion mit Emotet
  - Angriff per Email
- Montag – Mittwoch: diverse erfolglose Reinigungsversuche
- Mittwoch Nachmittag: Emotet-C2-Verbindungen fallen auf: **Alarm**
- Mittwoch Abend: kompletter Lockdown (inkl. Trennung vom Internet, Beschäftigte werden nach Hause geschickt)
- Ab Donnerstag: Analyse, Forensik mit externer Hilfe
  - über 100 infizierte Rechner
  - mind. 5 verschiedene Varianten von Emotet/Trickbot
  - AD hoffnungslos korrumpiert
- Ab Samstag: Wiederaufbau – komplett neu
  - Alle Rechner neu aufsetzen
  - Active Directory Domäne komplett neu aufbauen

- Glück im Unglück: Lockdown noch rechtzeitig vor Ryuk-Einsatz

Wie hoch schätzen sie den Schaden bei Heise?

A. **< 10.000 €**

B. **> 10.000 €**

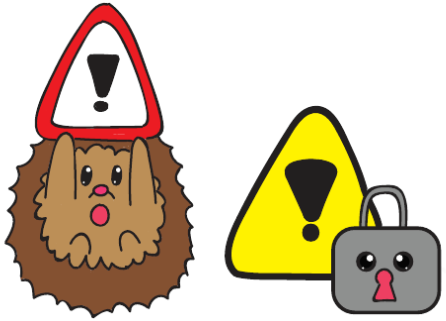
C. **> 50.000 €**

D. **> 100.000 €**

Folgen bei Heise

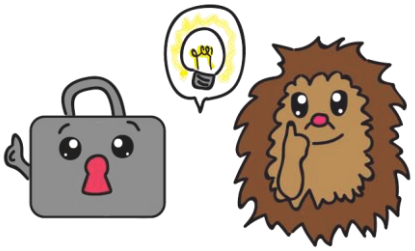
- Direkte Kosten:
  - Hardware + Beratung: ca **50.000 €**

- Dazu:
  - mehrere Tage Produktionsausfälle
  - Umsatzeinbußen
  - interne Arbeitskosten
  - Gesamtkosten nicht öffentlich bekannt



Lessons learned

- Hätte man es verhindern können?
  - Nein, nicht dauerhaft

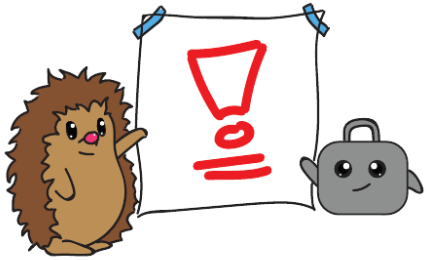


- Lehren, die Heise für sich zieht:
  - Es wird uns (wieder) treffen!
  - Es wird Infektionen und Kompromittierungen geben.
  - Teile unserer Schutzmaßnahmen werden versagen.
  - Es gibt keine einzelne „Silver Bullet for the win“.

- Eine sichere Firewall alleine reicht nicht (mehr)!

Grundlage: Bestandsaufnahme

- Schutzbedarfsanalyse
  - Klassifizieren Sie ihre Assets / Daten
  - Spezifizieren Sie Schutzziele
    - Verfügbarkeit
    - Integrität
    - Vertraulichkeit
    - …
- Synergien zu DSGVO
  - Datenschutzfolgeabschätzung



Verteidigungslinie 1: Awareness – aber richtig!

- Zunächst in der IT
  - „Ja, es wird uns treffen – und wir müssen da mehr tun“
- Dann im Management
  - „Ja, wir brauchen bessere Security – und wir müssen da investieren“
- Und dann auch: alle Mitarbeitende
  - „Ja, Security ist auch meine Aufgabe“

- Man kann es sich aussuchen:
  vorbeugend zahlen
  oder
  hinterher den Schaden bezahlen.

  Bezahlen muss man in jedem Fall.

  - Wer es vorher macht und damit auch nur die Folgen eines Einbruchs reduziert, hat die Kosten wieder drin.

Verteidigungslinie 2: Perimeter

- „Klassische“ Verteidigung
  - Firewall
  - Web-Filter
  - Mail-Filter
- Inhalte blockieren / Dinge als „verdächtig“ markieren
  - Office-Dateien in der Mail / als Download?
    - Braucht man die? Braucht die jeder?
    - Braucht man Dateien mit Makros? (einfach erkennen z.B. mit Yara https://github.com/Yara-Rules/rules/blob/master/Malicious_Documents/Maldoc_VBA_macro_code.yar)
    - Testen mit dem z.B. heise Emailcheck https://www.heise.de/security/dienste/Mails-mit-Anhaengen-777837.html
- Adressen
  - Domains im Anzeigename
    - “Hans Mustermann h.mustermann@tu-braunschweig.de“ <irgendwas@irgendwer.com>
    - „Hans Mustermann“ <h.mustermann-tu-braunschweig-de@my.com>
  - Interne Mails am externen Gateway von außen kommend
- Threat Intelligence / Indicators of Compromise (IoC) (Verkehr zu C2-Servern z.B.)

Verteidigungslinie 2: Perimeter - IoC

- Indicator of Compromise
- Quellen z.B.
  - Emotet Working Group / Cryptolaemus
    - https://paste.cryptolaemus.com/
  - URLhaus (abuse.ch)
    - https://urlhaus.abuse.ch/
  - FeodoTracker Dridex+Emotet+Trickbot
    - https://feodotracker.abuse.ch/

- Oder:
  entsprechende Appliances, die das ohne eigenen Programmier- und Wartungsaufwand liefern

Verteidigungslinie 3: Endpoint Security

- Standard:
  - Antiviren-Software,
  - regelmäßige Updates,
  - usw.
- Auf Emergency-Updates vorbereiten
- Systeme härten (Windows-Welt)
  - Alternativen wie Linux, LibreOffice?
  - Makros via Gruppenrichtlinie abschalten?
  - Whitelisting mit App-Locker / Software Restriction Policies?
  - Keine lokalen Admin-Rechte für Benutzer
  - Powershell Constrained Language Mode

- Auf Notfall-Recovery vorbereiten

Lehre: Admin-Rechte für Anwender sind wirklich BÖSE!

- Globale Policy, die das Arbeiten mit Admin-Rechten verbietet
- Meist gibt es aber Ausnahmen, natürlich gut begründete …
  - Organisatorisch
  - Software läuft nur, wenn Admin-Rechten erteilt werden
  - ….
- Bei Heise wurden **ALLE** diese Ausnahmen kompromittiert
- Also: **Keine Ausnahmen**!

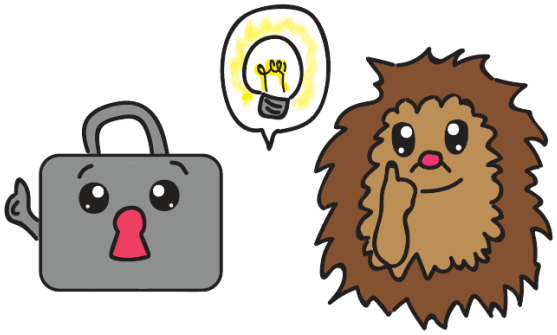
- Windows != Windows
  - Windows 7 Rechner wurden alle kompromittiert, aber nicht alle Windows 10-Rechner
- Security-Features, die Windows 7 nicht hat:
  - (Tiefe) Integration des Windows Defenders (ab Windows 8/10)
  - LSA (Local Security Authority) Protection (ab Windows 8)
  - Restricted Admin Mode für RDP (Windows 8)
  - Device Guard (Windows 10)

Credential Guard (Windows 10)

  - Windows Passport (Windows 10)

Verteidigungslinie 4: „das Netz“ + Active Directory

- Separation des Netzes in gut getrennte Bereiche
- Privilegien richtig verteilen und den Überblick behalten
- Active Directory
  - **Es wurden bei Heise keine (Software --) Schwachstellen ausgenutzt - Nur durch das Windows Betriebssystem bereitgestellte Funktionalitäten!**
  - Ausreichende Berechtigungen vorausgesetzt
- Häufiger Fehler: Überprivilegierte Konten
- Häufiger Fehler: zu viele Administratoren
- Häufiger Fehler: Administratoren melden sich mit dem selben Konto auf allen Ebenen an
- Häufiger Fehler: nicht mehr unterstützte (End-of-Life) Software / Systeme im Einsatz
- Häufiger Fehler: fehlendes Baseline Hardening
- Häufiger Fehler: kein AD-spezifisches Monitoring / Logging



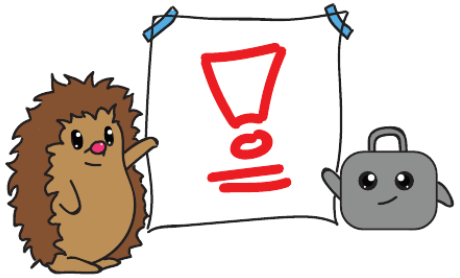
Lehre: AD / Windows Domänen - Härtung

- Strikte Anwendung des administratives Tier-Modells: Getrennte Admin-Konten für
  - Tier 0 (AD, Management Systeme)
  - Tier 1 (Anwendungsserver)
  - Tier 2 (Arbeitsplätze mit Internetzugang)
  - Tier 3 (Arbeitsplätze ohne Internetzugang)
- **Jede** Identität (Account) und **jedes System /Applikation** muss so klassifiziert werden, dass **es zu genau einem administrativen Tier** gehört.
- Identitäten eines höheren Tiers **muss** verboten werden, sich auf einem niedrigeren Tier anzumelden.
- Identitäten eines niedrigen Tiers dürfen **nicht** Identitäten, Systeme /Applikationen eines höheren Tiers kontrollieren.
- Implementiere das Clean Source Principle
  - Kontrollbeziehungen beachten (z.B. Installationsmedien)
  - Priviledged Access Workstations (PAW)
  - Segregation of Duties
- Passwort-Richtlinien, Patch-Management, Monitoring, Baseline Hardening (Server/Clients)

Verteidigungslinie 5: Monitoring

Es ist essentiell, dass man bemerkt, wenn man einen Vorfall hat!

- Monitoring
  - im Netz
  - auf Servern und
  - auf den Endpoints
- Suchen nach aktuellen IoCs (Indicators of Compromise)
- IDS (Intrusion Detection System) und SIEM (Security Information and Event Management Systeme) kann helfen
- aber **letztlich braucht man Menschen**
- Probleme:
  - viel (unproduktive) Arbeit
  - Fehlalarme
  - häufig gibt es Alarme, aber niemand beachtet sie
- Anregung:
  - Honeypots (Konten, Daten, Freigaben, die NIE benutzt werden) aufstellen und beobachten – Emotet ignoriert diese, aber ggf. fällt z.B. Trickbot dann auf



Verteidigungslinie 6: Backup / Recovery

Kein Backup: kein Mitleid!

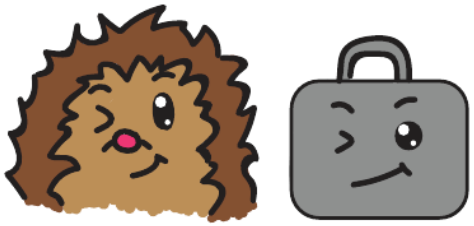
- Sind die Backups noch sicher, wenn ein Angreifer
  - gezielt danach sucht?
  - Admin-Rechte hat?
- Offline-Backups / Bänder
- Write Once Read Many (WORM)
- Regelmäßige Restore/recovery-Tests

Verteidigungslinie 7: Notfall-Vorbereitung

- Klären und **dokumentieren** (**offline** verfügbar!):
  - Zuständigkeiten
  - Ansprechpartner
  - Erreichbarkeit
  - Abläufe bei Vorfällen – Notfallpläne
  - Sind die Notfallpläne auch aktuell?
- Üben der Abläufe – regelmäßige Notfall-Trainings
- Vorbild aus der analogen Welt: regelmäßige Feueralarm-Übungen

Fazit (nicht nur) bei Heise

- **Gehen Sie davon aus, dass Sie in den nächsten 3 - 6 Monaten einen Emotet-Vorfall haben werden.**
- **Und wenn nicht Emotet, dann einen anderen.**
- **Es gibt 2 Typen von Organisationen: die, die gehackt wurden – und die, die noch nicht wissen, dass sie gehackt wurden.**
- Was passiert, wenn Ihre Verteidigungselemente fallen? (Resilienz erhöhen!)
  - Filter
  - Awareness
  - AV
  - Trennung User/Admin
  - ...



- Priorisierung der Maßnahmen:
  - Wo sind die Schwachpunkte in Ihrem Security-Konzept?
  - Was sind Ihre „Kronjuwelen“?

Was nehmen sie aus diesem Vortrag mit?

Offene Diskusion!

Weitere Infos:
https://doku.rz.tu-bs.de/doku.php?id=it-sec:it-sec und
http://it-sicherheit.tu-braunschweig.de/

https://pixabay.com/de/baby-lernen-laptop-frage-2709666/
CC0 Lizenz

und beim IT-Service-Desk des Gauß-IT-Zentrums
Tel. +49.531.391.55555
it-service-desk@tu-braunschweig.de **https://www.tu-braunschweig.de/it/service-desk**

Vielen Dank für Ihre Aufmerksamkeit!