Erfahrungen mit Emotet an der Universität Duisburg-Essen

Kontakt:
andreas.bischoff@uni-due.de
marius.mertens@uni-due.de

54. Sitzung des AK-IT der Leibniz-Gemeinschaft
19.11.2020 // Dr. Andreas Bischoff und Dr. Marius Mertens

Basiert auf…

Sept. 2019, DFN Betriebstagung
mit Inga Scheler (TU Kaiserslautern)

Inhalt

- Angriffsvorbereitung bis zur Angriffsmail
  → Live-Hacking A. Schinner
- **Auswirkungen der Angriffsmail**
  - Fähigkeiten und Verbreitung
  - Ablauf der Infektion
  - Erkennung und unmittelbare Reaktion
- Datenabfluss und nachgelagerte Angriffsvektoren
  → Live-Hacking A. Schinner
- Reparatur und Härtung der IT

Was ist (nicht nur) Emotet?

- Bekannt seit (mindestens) 2014
- Dropper für eigentliche Malware (ursp
- Fortschrittliche Defensivmechanismer
  - Polymorph → Signaturbasierte Viren
  - Sandboxerkennung
- Fortschrittliche Offensivmechanismen
  - Stehlen von Credentials: Bruteforce
  - E-Mail Exfiltration
  - Nutzen bekannter Exploits
- Modularer Aufbau
  - Trickbot: Bankingtrojaner (Vorläufer
  - Mimikatz: Stiehlt Kerberos-Tickets
    Achtung: 2FA hilft dagegen nicht! Vi
    (Neukompilierung für jeden möglich
- Command & Control Server für Befeh
- Atombombe für die Hosentasche

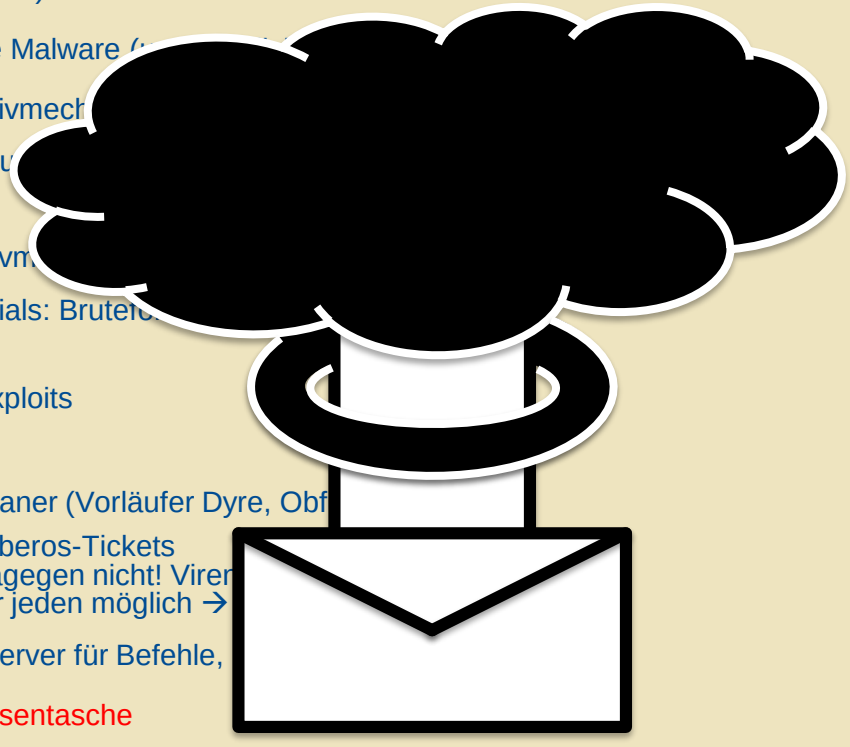
Was ist (nicht nur) Emotet?

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

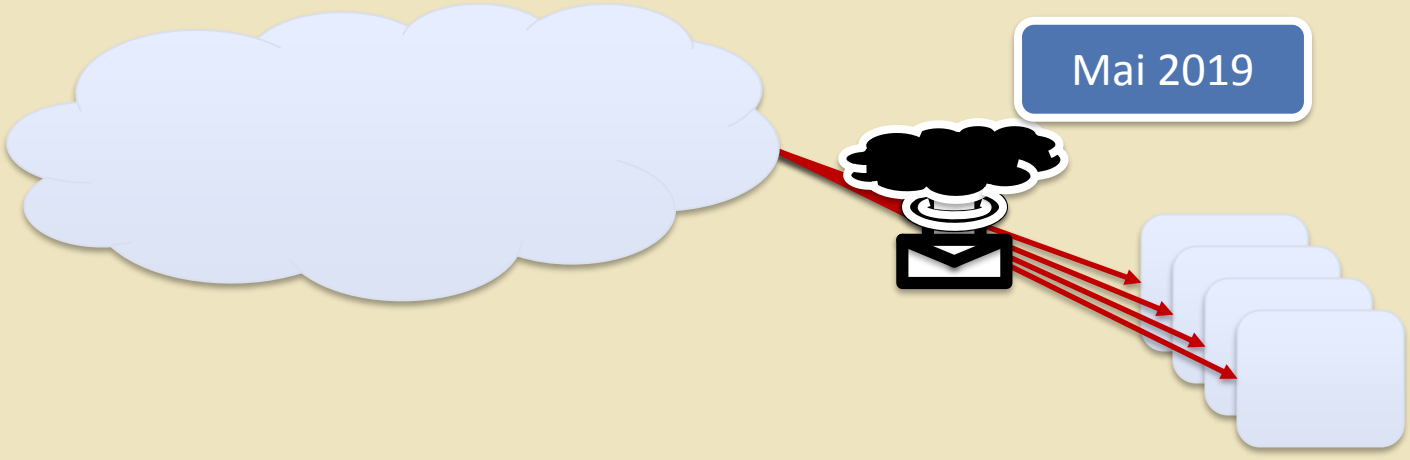
- Bekannt seit (mindestens) 2014
- Dropper für eigentliche Malware (ursprünglich Banking-Trojaner)
- Fortschrittliche Defensivmechanismen
  - Polymorph → Signaturbasierte Virenscanner versagen oft
  - Sandboxerkennung
- Fortschrittliche Offensivmechanismen
  - Stehlen von Credentials: Bruteforce, Keylogger
  - E-Mail Exfiltration
  - Nutzen bekannter Exploits
- Modularer Aufbau
  - Trickbot: Bankingtrojaner (Vorläufer Dyre, Obfuscation)
  - Mimikatz: Stiehlt Kerberos-Tickets
    Achtung: 2FA hilft dagegen nicht! Virenscanner nur bedingt
    (Neukompilierung für jeden möglich → liegt bei Github)!
- Command & Control Server für Befehle, Updates, Payload
- Atombombe für die Hosentasche

Was ist (nicht nur) Emotet?

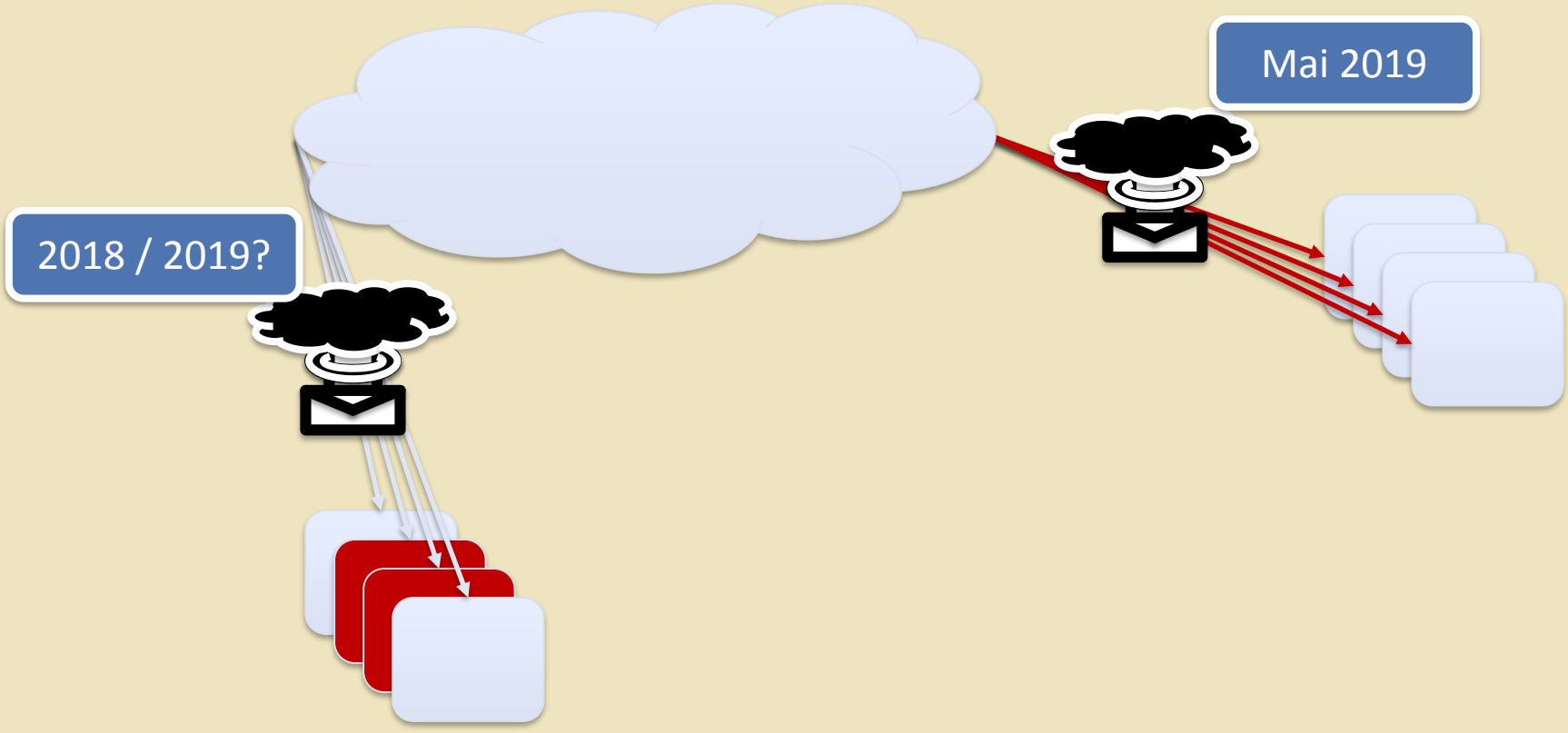
- Bekannt seit (mindestens) 2014
- Dropper für eigentliche Malware (
- Fortschrittliche Defensivmech
  - Polymorph → Signatu
  - Sandboxerkennung
- Fortschrittliche Offensivm
  - Stehlen von Credentials: Brutef
  - E-Mail Exfiltration
  - Nutzen bekannter Exploits
- Modularer Aufbau
  - Trickbot: Bankingtrojaner (Vorläufer Dyre, Obf
  - Mimikatz: Stiehlt Kerberos-Tickets
    Achtung: 2FA hilft dagegen nicht! Viren
    (Neukompilierung für jeden möglich →
- Command & Control Server für Befehle,
- Atombombe für die Hosentasche



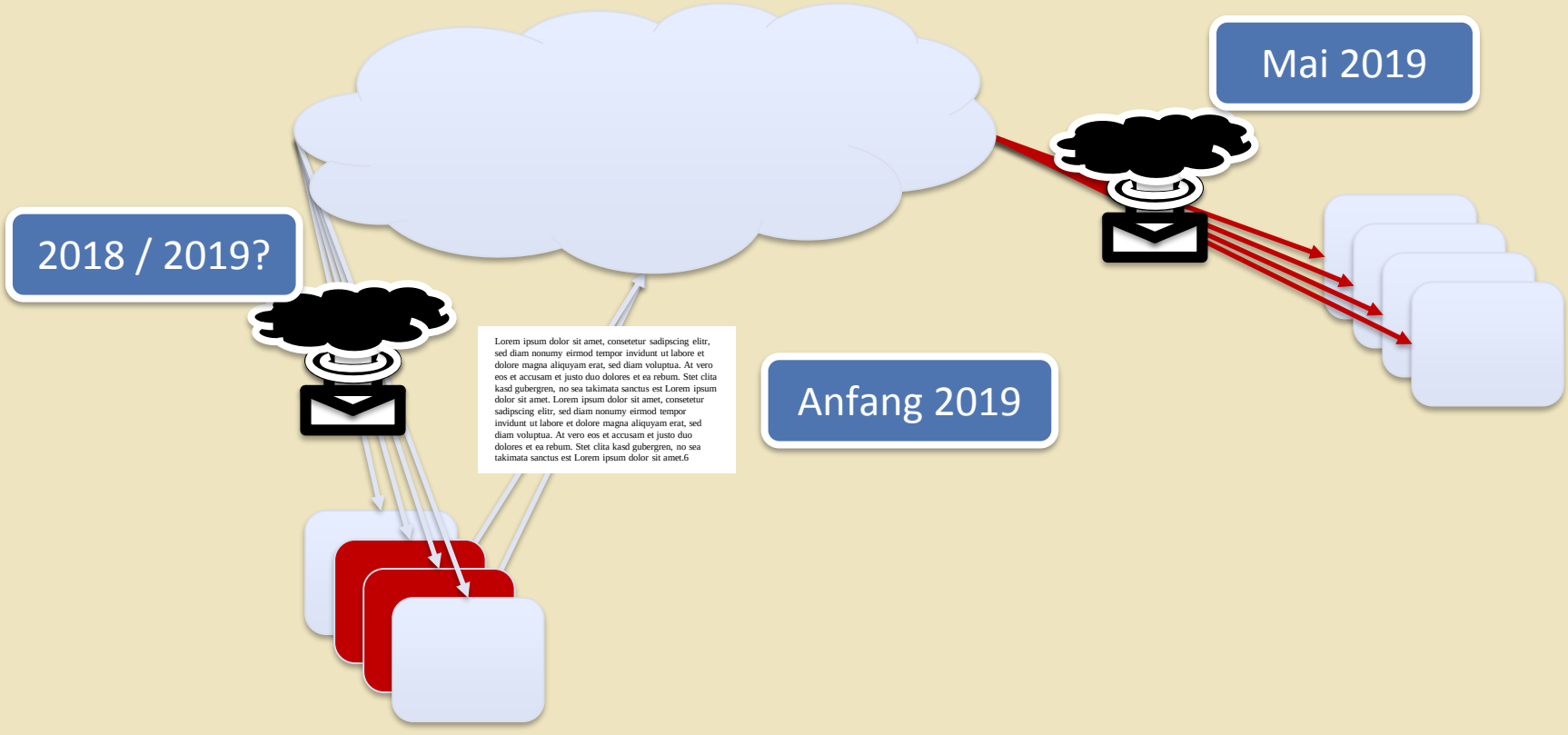
Ablauf der Infektion



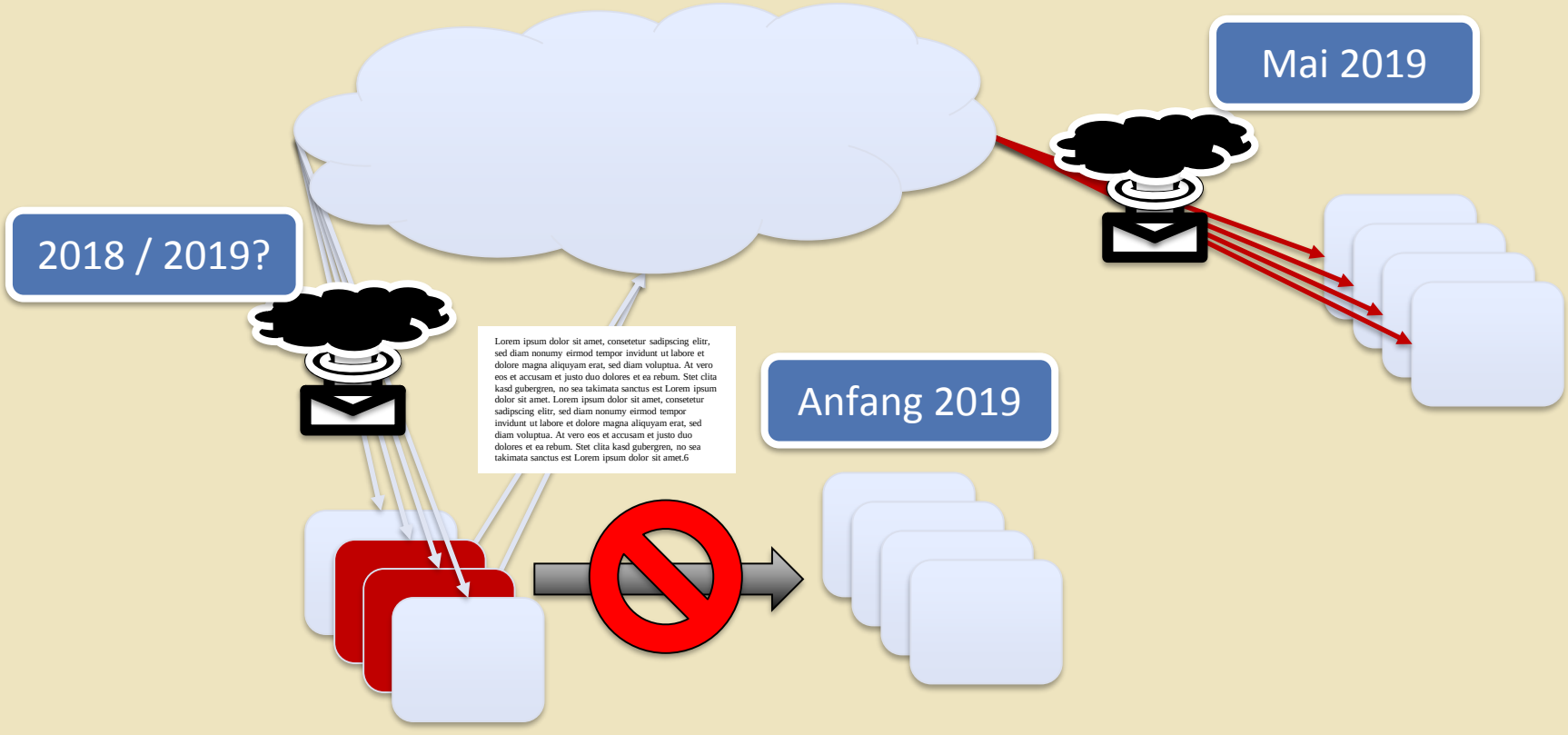
Ablauf der Infektion



Ablauf der Infektion



Ablauf der Infektion



Ablauf der Infektion

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

14.05.2019

15:43: Erste Emotet-Angriffsmail mit zuvor exfiltriertem Inhalt entdeckt

15:55: Erste Nutzermeldung eingehender Angriffsmails an CISO

15:55: CISO informiert ZIM-CERT über den Angriff

16:08: Vorbereitung einer Sicherheitsmeldung (RSS-Feed)

16:32: Sicherheitsmeldung online

17:15: Eingang weiterer Meldungen; Isolation von „Patient 0“

17:55: Unabhängige Warnung an „Patient 0“ von designiertem Opfer

Ablauf der Infektion

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

15.05.2019: Virenscan „Patient 0“ ohne Befund. PC wurde neu aufgesetzt, AD Profil gelöscht, Kennwörter geändert.
Information des Datenschutzbeauftragten über eventuell meldepflichtigen Vorfall
16.05.2019: Entscheidung DSB: Vorfall ist meldepflichtig
17.05.2019: Meldung beim LDI und Information aller MitarbeiterISO informiert ZIM-CERT über den Angriff
22.05.2019: Welle der Angriffsmails ebbt ab. Insgesamt 5 zuvor infizierte PCs identifiziert und bereinigt. Kein Anzeichen erfolgreicher lateraler Verbreitung (aber man kann niemals völlig sicher sein…)

Ablauf der Infektion

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Juni 2019: Rektoratsbeschluss: Legacy-Office-Sperre, Infomail, Schulungen

Juni 2019: (Signierte!) Informationsmail an alle Hochschulangehörigen

Juli 2019: Mails mit Legacy-Office-Dokumenten werden nicht mehr angenommen, der absendende Server wird Mail nicht los

Dezember 2019: Sicherheitsvorfall JLU Gießen

Dezember 2019: Sicherheitsvorfall Uni Maastricht (Kundenbetreuung!)

Mai 2020: Deutlich erhöhtes Aufkommen Angriffsmails mit Legacy-Office-Anhängen

Mai 2020: Sicherheitsvorfall Ruhr-Uni Bochum

September 2020: Sicherheitsvorfall Uniklinik Düsseldorf

Indicators of Compromise

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- Typische E-Mails mit originalen Inhalten und Malware im Anhang von (externen) gefälschten Absendern
- Externe Meldungen von Spamversand aus der UDE (trotz gefälschter Absender)
- **Nicht beobachtet: Verschlüsselungsaktivitäten oder Erpressungsversuche**
- Was hätten wir beobachten können (Netzwerküberwachung):
  - Versuche der lateralen Verbreitung per SMB
  - Verbindung zu C2-Servern


UNIVERSITÄT
DUISBURG
ESSEN
Offen im Denken

- Angriffsvorbereitung bis zur Angriffsmail
  → Live-Hacking A. Schinner
- Auswirkungen der Angriffsmail
- **Datenabfluss und nachgelagerte Angriffsvektoren**
  → Live-Hacking A. Schinner
- Reparatur und Härtung der IT


UNIVERSITÄT
DUISBURG
ESSEN
Offen im Denken

- Angriffsvorbereitung bis zur Angriffsmail
  → Live-Hacking A. Schinner
- Auswirkungen der Angriffsmail
- Datenabfluss und nachgelagerte Angriffsvektoren
  → Live-Hacking A. Schinner
- **Reparatur und Härtung der IT**
  - Technische Maßnahmen
  - Organisatorische Maßnahmen
  - Lessons learned
  - Empfehlungen

Retrospektive

- **Mögliche Zustände „nach“ Emotet**
  - Wir haben unser AD neu aufgesetzt und alle alten Rechner entsorgt
  - Wir haben offensichtlich befallene PCs neu installiert und die Nutzer haben ihre Passwörter geändert
  - Ähhh, Lasagne?

Unmittelbare Reaktion

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- **Unternehmensweite Warnung an**
  - Infizierte Nutzer
  - Nicht infizierte Nutzer
  - Administratoren (nicht auf infizierten Rechnern anmelden)
- **Isolation aller infizierten Rechner**
- **Ggf. Beweissicherung / Forensik**
- **Vollständiges Löschen aller infizierten Rechner (UEFI)**
- **Vollständiges Löschen aller infizierten AD-Profile**
- **Passwörter aller Accounts aller betroffenen Nutzer zurücksetzen**
- **Strafanzeige erstatten**
- **Bericht an Landesbeauftragte für Datenschutz und Informationsfreiheit (DSGVO)**

Vorbeugende Maßnahmen

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- Vorgesetzte mit S-MIME-Zertifikat ausgestattet
  - Vorbildfunktion
  - Stark verbreitete S-MIME-Signatur in der Hochschulverwaltung
- Crypto-Partys in den Abteilungen der Hochschulverwaltung
- **Infomail durch RZ-Leiter an alle Hochschulangehörigen**
  - **Sperrung der Legacy-Office-Formate**
  - **Phishing-Warnung**
  - **Information über meldepflichtigen Datenschutzvorfall**
- **Sperrung der Legacy-Office-Formate (allerdings nicht sofort, sondern erst nach erneutem Gremien-Lauf per Rektoratsbeschluss)**
- Verpflichtende Awareness-Schulung für alle Mitarbeiter
- Nicht vergessen: Auch von mittlerweile bereinigten Rechnern wird die abgegriffene Kommunikation weiterhin für Angriffe verwendet!

E-Mail-Signatur und Zertifikate

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- **Die allermeisten Probleme bei E-Mails lösen sich durch digitale Signaturen**
- **Zertifikat beantragen: https://pki.pca.dfn.de/uni-duisburg-essen-ca-g2/pub**
- **Anleitung: https://www.uni-due.de/zim/services/e-mail/konfigurationsanleitungen/zertifikat-anfordern**
- Kleines „aber“
  - Der Einrichtung von Zertifikaten ist etwas umständlich (Identitätsüberprüfung mit Personalausweis → Corona)
  - Wiederherstellung des Zertifikats?
  - Umgang mit verschlüsselten Mails?
  - **Admins oder ZIM fragen!**

„Nach“ Emotet

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- **Nicht vergessen: Auch von mittlerweile bereinigten Rechnern wird die abgegriffene Kommunikation weiterhin für Angriffe verwendet!**
- **Gibt es weitere infizierte Rechner?**
- **Sind Administratorkennwörter kompromittiert?**
- **Redesign des Active Directory**
- **(Unsignierte) Makros auf allen Rechnern blockieren**
- **Gefährliche E-Mail-Anhänge blockieren**
- **Verbesserte Detektion (im Netzwerk und an Endpunkten)**

Empfehlungen – technisch

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- ALLE Passwörter, die auf befallenen Rechnern jemals benutzt wurden, ändern (auch gespeicherte Passwörter im Browser)
- 3-Tier-Adminkonzept für AD
- Diversität in der IT hilft
- Datensicherung hilft immer

KEIN BACKUP?
KEIN MITLEID!

- E-Mail-Sicherheit: Signaturen, Markierungen (extern?), selbst „richtig“ E-Mails schreiben
- Administratoren: Desaster Recovery vorbereiten und üben

Empfehlungen – organisatorisch

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- **Lokales CERT**
- **Nutzer melden Spam und Phishing an spezielle E-Mail-Adresse**
- **Kommunikationskanal zu den Nutzern**
  - Mehrsprachig
  - Sicherheits-RSS-Feed (wird von dezentralen Admins sogar gelesen) mit u.a. regelmäßigen Spam-Warnungen
  - Website
  - (Massen-)E-Mail ist problematisch, wenn dann nur signiert
- **CISO**
- **Informationssicherheitsrichtlinie**
- **Dezentrale Informationssicherheitsbeauftragte**
- **Sensibilisierungsmaßnahmen – notfalls verpflichtend**

Lessons Learned

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- **Infizierte Accounts nur durch exfiltrierte Inhalte aufgefallen**
  - Gibt es weitere unentdeckte Infektionen?
  - Welche weiteren Zugangsdaten könnten kompromittiert sein?
  - Läuft der nächste unauffällige Angriff bereits?
- **Maßnahmen sind (organisatorisch) schwer umzusetzen, bevor etwas passiert**
- **Information ist essentiell, aber es ist schwer, alle Beteiligten zu erreichen**
- **„Networking“ ist wichtig: Informationsaustausch über Angreifer, größere Kampagnen, etc.**

Was furchtbar schiefgehen kann…

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

- Initiale Infektion auf kritischem Rechner
- Remotezugriff aktiv und schwache Kennwörter
- Nicht alle (Sicherheits-)Updates installiert
- Anmeldung AD (DC) Administrator auf infiziertem Rechner

- Vorbeugung: Obiges verhindern!
  … und aktuelles Backups haben (offline)
  … und Backups getestet haben
  … und wissen wie Restore funktioniert

Fazit

- **Meldewege vorbereiten, kommunizieren, üben**
  - Spamverdacht? Nutzer => IT
  - Bedrohungslage? IT => Nutzer
  - Awareness / Schulungen (Nutzer und Admins): Wichtig, aber nicht ausreichend
- **Technisches**
  - Security by Design → Reguläre Nutzer sollten keinen Schaden anrichten können
  - Diversität nutzen
- **Durchführung von Maßnahmen**
  - Rückhalt bei Leitung und Gremien suchen → Es gibt immer Widerstand
  - Befugnisse und Verantwortlichkeiten im Vorfeld regeln
- **Empfehlungen für Leiter**
  - Sicherheitsmaßnahmen mittragen und vertreten (auch gegen chronische Meckerer)
  - Auf das Sicherheitsteam hören, bevor es wehtut

Fazit

- **Meldewege vorbereiten, kommunizieren, üben**
  - Spamverdacht? Nutzer => IT
  - Bedrohungslage? IT => Nutzer
  - Awareness / Schulungen (Nutzer und Admins): Wichtig, aber nicht ausreichend
- **Technisches**
  - Security by Design → Reguläre Nutzer sollten keinen Schaden anrichten können
  - Diversität nutzen
- **Durchführung von Maßnahmen**
  - Rückhalt bei Leitung und Gremien suchen → Es gibt immer Widerstand
  - Befugnisse und Verantwortlichkeiten im Vorfeld regeln
- **Empfehlungen für Leiter**
  - Sicherheitsmaßnahmen mittragen und vertreten (auch gegen chronische Meckerer)
  - Auf das Sicherheitsteam hören, bevor es wehtut

Fazit

- **Meldewege vorbereiten, kommunizieren, üben**
  - Spamverdacht? Nutzer => IT
  - Bedrohungslage? IT => Nutzer
  - Awareness / Schulungen (Nutzer und Admins): Wichtig, aber nicht ausreichend

Ausblick: Emotet war erst der Anfang, die Atombombe für die Hosentasche wird für jeden Angreifer verfügbar
Neue Anwendung für Passwortklau: Übernahme aller Nutzeraccounts (Mail, Cloud, soziale Medien) und Freigabe gegen Bitcoins
Weitere Angriffsvektoren: Übernahme von IoT und Smartphones

  - Sicherheitsmaßnahmen mittragen und vertreten (auch gegen chronische Meckerer)
  - Auf das Sicherheitsteam hören, bevor es wehtut

Fazit

- **Meldewege vorbereiten, kommunizieren, üben**
  - Spamverdacht? Nutzer => IT
  - Bedrohungslage? IT => Nutzer
  - Awareness / Schulungen (Nutzer und Admins): Wichtig, aber nicht ausreichend

Ausblick: Emotet war erst der Anfang, die Atombombe für die Hosentasche wird für

Vielen Dank für Ihre Aufmerksamkeit!

  - Sicherheitsmaßnahmen mittragen und vertreten (auch gegen chronische Meckerer)
  - Auf das Sicherheitsteam hören, bevor es wehtut