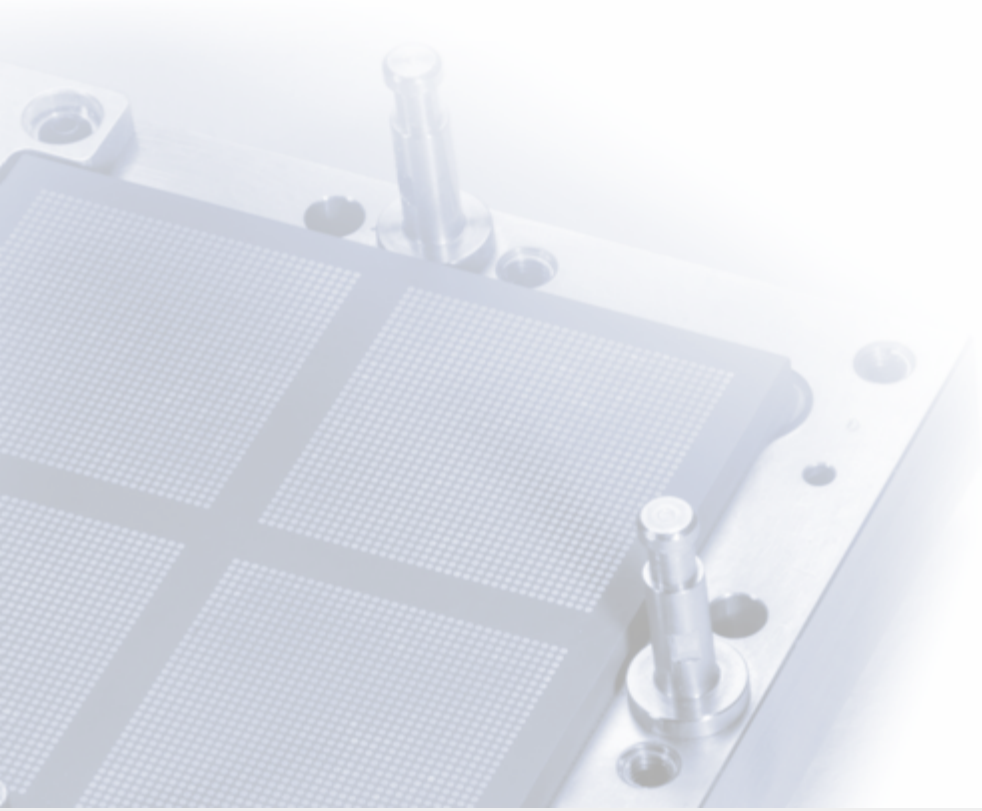
Leibniz Universität Hannover

Zur Sicherheitslage

Hergen Harnisch
harnisch@luis.uni-hannover.de



„Das Problem liegt in der Kombination von wachsender Gefährdung mit zunehmender Abhängigkeit von Informationstechnik.

Die Wahrscheinlichkeit für den Erfolg von Angriffen auf digitalisierte Infrastrukturen steigt, da

1. sich die Anzahl der Angriffspunkte erhöht,
2. die Kommunikationsinfrastrukturen immer komplexer werden und
3. die zu verarbeitenden Datenmengen sich vervielfachen."

(nach BSI-Lagebericht 2018)

$\Longrightarrow$ Digitalisierung benötigt mehr IT-Sicherheit

— oder Vorbereitung auf Alternativen

Programm

Dienstag 17.11.15

13:15-14:45 Sicherheitslage
14:45-15:15 *Pause*
15:15-16:45 Linux-Firewalling

Mittwoch 18.11.15

09:15-10:45 Awareness
10:45-11:15 *Pause*
11:15-12:45 TLS & PKI

Lagebild

Vorfälle:

- malicious Spam / Phishing
- Emotet
- Veranstaltungsmanagement
- Data-Leakage

Lagebild

Zahlen?

„Die Zahlen klingen dramatisch: 800 Millionen Schadprogramme im Umlauf, 390.000 neue Varianten pro Tag, 16 Millionen Warnmails verschickt. Wer den Jahresbericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) liest, möchte am liebsten seinen Computer für alle Zeiten ausschalten." (golem.de)

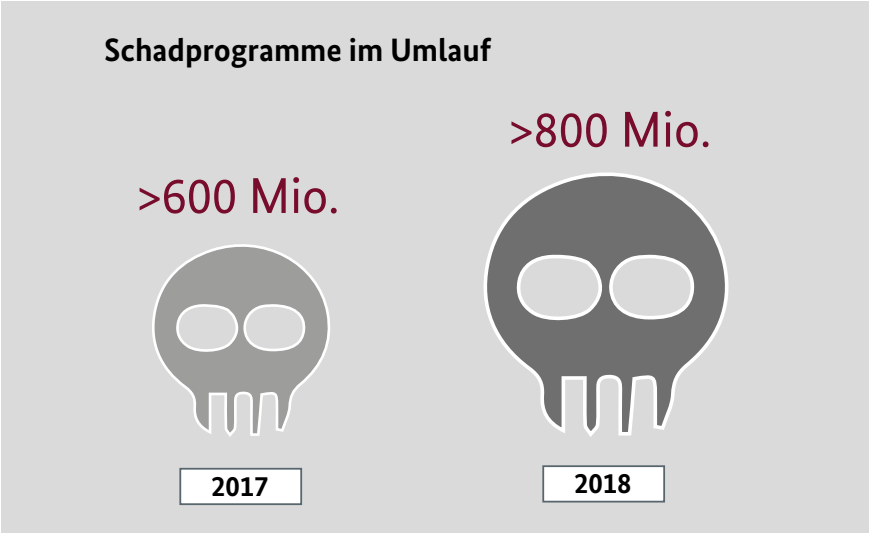
Bei „Sicherheitsvorfall" fehlt brauchbare Definition & Zählweise

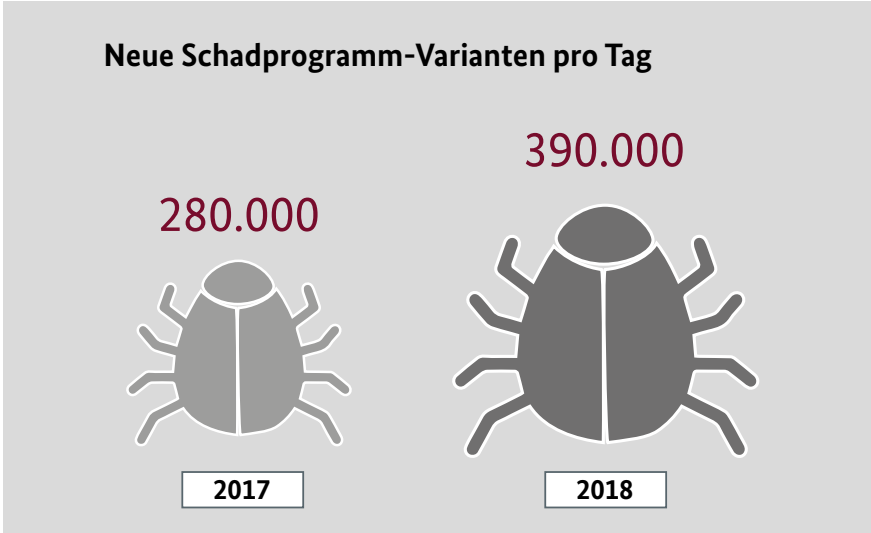
- qualitativ zählt schon ein Drop an der Firewall?
- quantitativ Zählweise abh. vom Schaden (ein Client vs. ganzes Institut)
- unbekannt unaufgedeckt & ungemeldete Sicherheitsvorfälle

$\Longrightarrow$ *Zahlen nur bedingt aussagekräftig, dienen meist Ziel …*

Lagebild

Schadprogramme





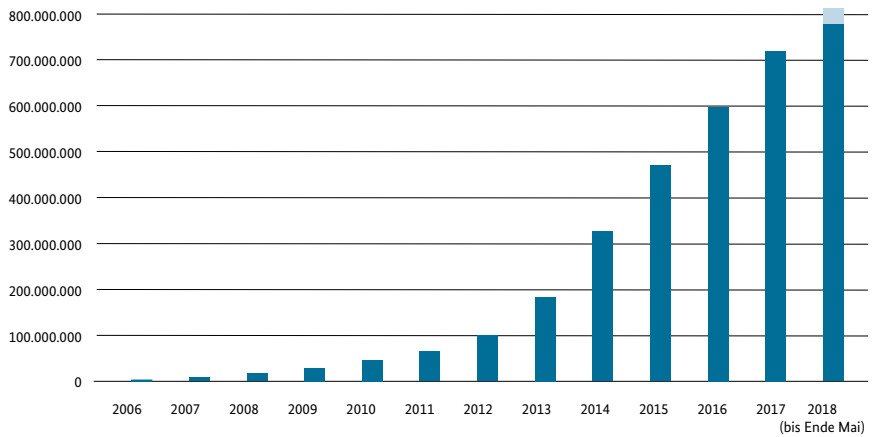


Abbildung 12 Bekannte Schadprogramme, Quelle: AV-Test, Stand: 31.05.2018

(aus BSI-Lagebericht 2018)

- Varianten z.B. bei Spam
- AV mit Hashes unzureichend

Lagebild

LUH: Warn-/Vorfallsmeldungen DFN-Cert

219 Mails des DFN-CERT zu Vorfällen und Sicherheitslücken in 2018:

- 212 als automatische Warnmeldung:
  Meldung über CERT-Verbund, Sensornetze / Honeypots
- 7 vom DFN händisch bearbeitete
  - 2 Mails zu ausgehobenen Bot-Netzen mit Credentials
  - 2 Mails zu Phishing (Phishing-Kampagne, Spear-Phishing)
  - 3 Mails zu offenen Sicherheitslücken

Meldungen je Tag in 1-6 Mails,
Fast alle Meldungen sind 1- Vorfälle,
beziehen sich auf IP-Adressen oder Nutzerkennungen

Lagebild

LUH: DFN-Mails nach IP-Adressen

1.156 gemeldete IP-Adressen der LUH in 2018:

- 593 = 558 `Bot/HTTP` + 35 `Bot`
  Bots, d.h. durch Dritte kontrollierte IT-Systeme
- 471 `Attack/Malware` Angriffsursprünge
- 78 `Configuration/Amplifier`
  Fehlkonfiguration mit Amplifikation-Problem (z.B. DNS, NTP)
- 14 `Configuration/Unrestricted access`
  uneingeschränkter Zugriff auf sensiblen Dienst

IP-Adressen teilweise zeitlich versetzt mehrfach auffällig,
seltener ein Gerät mit geänderter IP (z.B. WLAN, VPN),
nur Einzelfälle false positive

Lagebild

Veränderungen der Gefährdungslage

„Die Gefährdungen sind im Berichtszeitraum im Vergleich zum vorangegangenen Berichtszeitraum vielfältiger geworden. “

(BSI-Lagebericht 2018)

Angriffstechnik

- HW-Probleme wie Spectre  & Meltdown 
- Kompromitierung von Installations- & Update-Quellen
- z.B. Emotet (s.u.)
- IoT-Botnets (z.B. Mirai)

Zweck

- zunehmender Handel mit Credentials (Identitätsdiebstahl)
- DDos-Erpressung (Q1/2018: bis 190 Gbit/s in Deutschland)
- Krypto-Mining

Lagebild

Wissenschaftsspionage

Spiegel-Online 20.4.2018

Spionage-Ermittlungen

Iranische Hacker attackieren 23 Hochschulen in Deutschland

"Hier klicken, sonst läuft Ihr Bibliothekszugang aus": So haben sich iranische Hacker nach SPIEGEL-Informationen Zugang zu Uni-Dokumenten verschafft, auch in Deutschland. Die Behörden ermitteln, die Attacke läuft weiter.

http://spon.de/afdm5, auch Spiegel 17/2018

Warnung Verfassungsschutz u.a. ca. 10/2018

Nds. Verfassungsschutz warnte vor (einfacher) Phishing-Kampagne

- anderer Staat mit Absicht Wissenschaftsspionage gegen dt. HSen
- einfache Angriffsmethoden als „harmloser" 1. Schritt

Lagebild

Advanced Persistent Threads

Regierungseinrichtungen	Militär/Rüstung	Opposition	Medien	Energie	Finanzen	Telko	NGO	Universitäten	High-Tech	Transport/Logistik	Luft- und Raumfahrt	Gesundheit	Kanzleien
APT12/ NumberedP. APT28/ Sofacy APT29/ CozyBear APT32/ OceanLotus APT37/ Reaper Bahamut BlueMushroom Cadelle/ Chafer Callisto CharmingKitten DarkCaracal DarkHotel DroppingElephant EmissaryPanda ExtremeJackal Gamaredon	APT28/ Sofacy APT37/ Reaper AridViper BlueMushroom Callisto CharmingKitten C-Major/ PureStrike DarkCaracal DroppingElephant Gamaredon GazaCybergang HammerPanda HelixKitten LotusPanda Machete Naikon/ OverrideP. Leviathan OilRig Operation-	Ahtapot APT32/ OceanLotus Bahamut BlackOasis Bookworm CharmingKitten DarkCaracal EnergeticBear FlyingDragon Group5 Infy Neodymium Operation-Cleaver Operation Manul Promethium ScarCruft Sima Stealth-Falcon SunTeam Temper-	APT28/ Sofacy APT32/ OceanLotus Bahamut BlackOasis BugDrop Callisto CharmingKitten DarkCaracal DarkHotel DroppingElephant GazaCybergang Infy Olympic-Destroyer Operation Manul Sandworm ScarCruft Shrouded-Crossbow Stealth-Falcon SunTeam Tick	APT10 APT18/ Wekby APT29/ CozyBear CharmingKitten ElectricPowder EmissaryPanda EnergeticBear GazaCybergang Greenbug HelixKitten Kraken/ Laziok Longhorn Machete MuddyWater OnionDog Operation-Cleaver Sandworm Shamoon Tropic-Trooper/ PirateP.	APT18/ Wekby APT29/ CozyBear BlueMushroom DarkCaracal DroppingElephant EmissaryPanda EnergeticBear EquationGroup GazaCybergang HammerPanda Longhorn OilRig Sandworm	APT18/ Wekby Codoso EmissaryPanda HammerPanda HelixKitten Longhorn Machete MuddyWater OilRig ProjectSauron Thrip	APT29/ CozyBear APT37/ Reaper Callisto CharmingKitten DarkHotel HammerPanda Honeybee Infy NilePhish Operation-Cleaver RocketKitten	APT10/ menuPass BugDrop CharmingKitten Codoso DarkCaracal DarkHotel Greenbug DarkHotel Longhorn Leviathan RocketKitten	APT18/ Wekby CharmingKitten Codoso LEAD/ Winnti Tick	Cadelle/ Chafer NanHaiShu OilRig OnionDog ProjectSauron Shamoon	APT28 DroppingElephant EmissaryPanda Leviathan HammerPanda Greenbug Longhorn	APT10/ menuPass Leviathan LEAD/ Winnti	APT29/ CozyBear Codoso DarkCaracal DeepPanda Leviathan

Berichte über APT-Gruppen je Branche (BSI-Lagebericht 2018)

$\Longrightarrow$ reale Bedrohung auch für die Wissenschaft

Lagebild

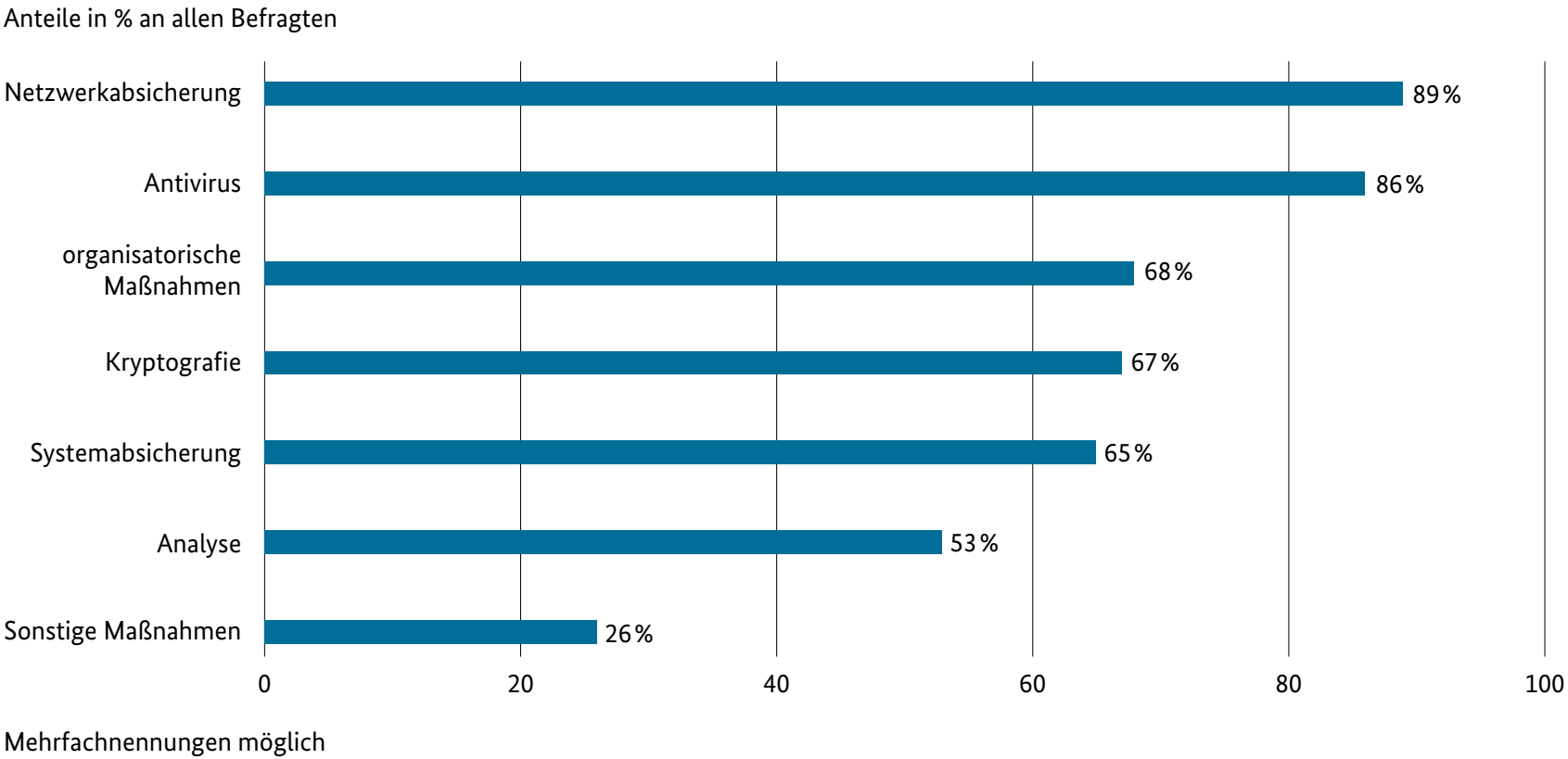


Abbildung 04 Welche Maßnahmen werden aktuell in Ihrer Institution zum Schutz gegen Cyber-Angriffe umgesetzt?

Lagebild

Gateway-Security

+ Firewall relativ leicht umsetzbar
- wenig wirksam gegen aktuelle Angriffe (und abnehmend)
o wirksam nur bei dedizierten Sicherheitsgateways (z.B. Mail)

Leider nochimmer verbreitete Meinung: „durch Firewall gesichert“

Vertrauen Sie nicht Ihrem LAN,
nutzen Sie IP-Adressen nicht als Autentifizierung!

Vorfälle: malicious Spam / Phishing

- Grenzen zwischen Spam und Phishing verwischen,
  bösartige Anhänge oder Verweise auf bösartige Websites

$\Longrightarrow$ „malicious spam“,
Spam-Abwehr wächst von Arbeitsenlastung zu
wichtiger, echter Sicherheitsmaßnahme

- vor ein paar Jahren Spam-Flaute, nun deutlich zunehmend
- Versand weniger über Bots, mehr gehackte Credentials
- neben alten Dingen wie Partnervermittlung oder Medikamenten
  nun bessere Texte, teils zielgerichtet. Z.B.
  - Bewerbungen
  - CEO-Fraud
- Angriffsvektor: technische Lücken, mehr aber Social-Engineering

Datei Bearbeiten Ansicht Navigation Nachricht Enigmail Extras Hilfe

Von Raimund Fraatz <> ☆ | Antworten | Allen antworten | Weiterleiten | Mehr

Betreff **Raimund Fraatz Rechnung CID609508 vom 06.11.2018** 06.11.18, 05:59

An ml@fzk.uni-hannover.de ☆

Sehr geehrte(r),

Raimund Fraatz Order U191076842
Kunden RS2452
Datum 06/11/2018
Rechnung CID609508

Zwischensumme (netto) 852,00 € inkl. Mwst 161,88 €
Einzelpreis (brutto) 1013,88 €

Versandart: DHL
Lieferdatum: Ist gleich dem Rechnungsdatum.
Vielen Dank für Ihren Einkauf!

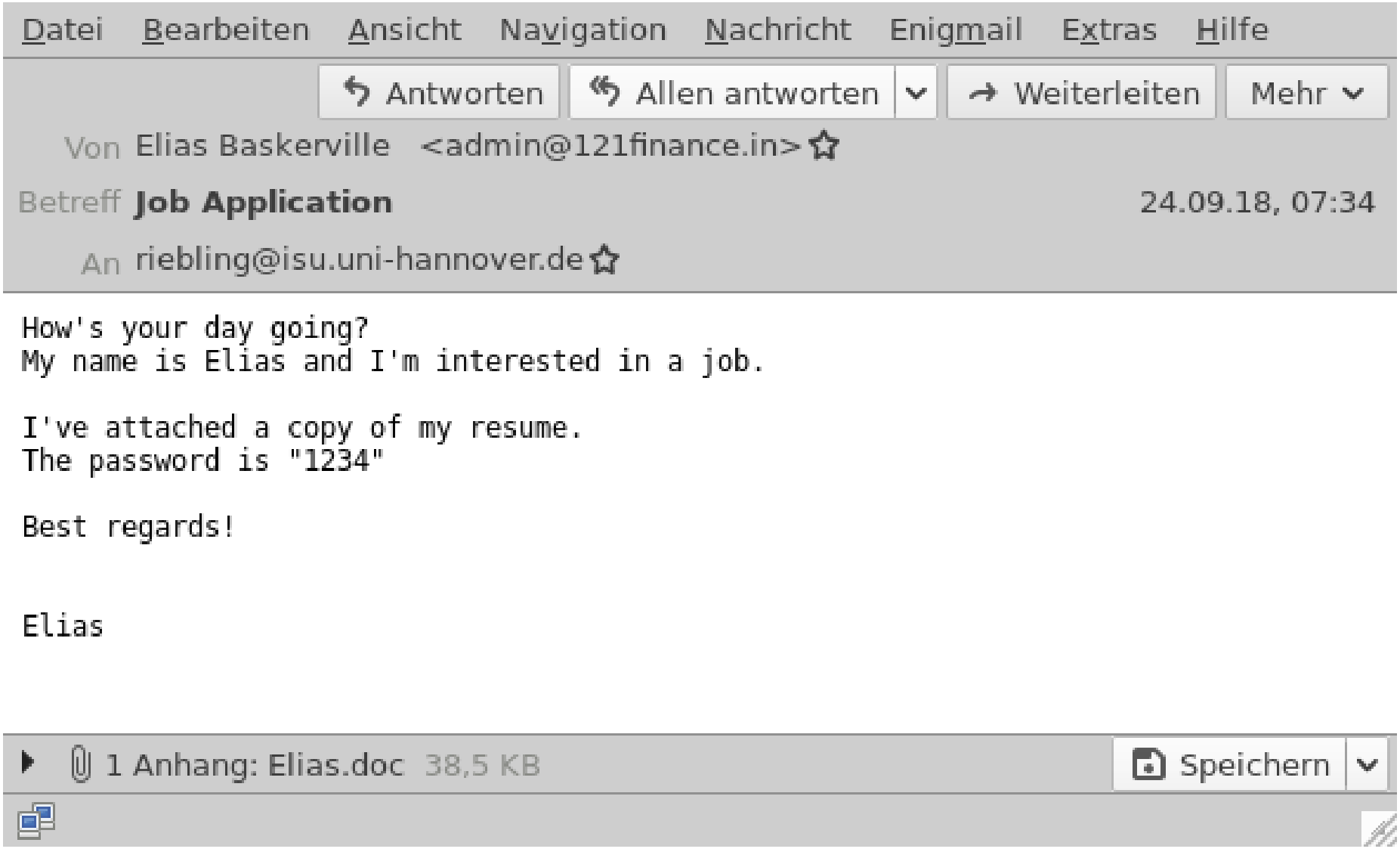
Wir freuen uns auf die weitere Zusammenarbeit mit Ihnen.

Freundliche Grüße

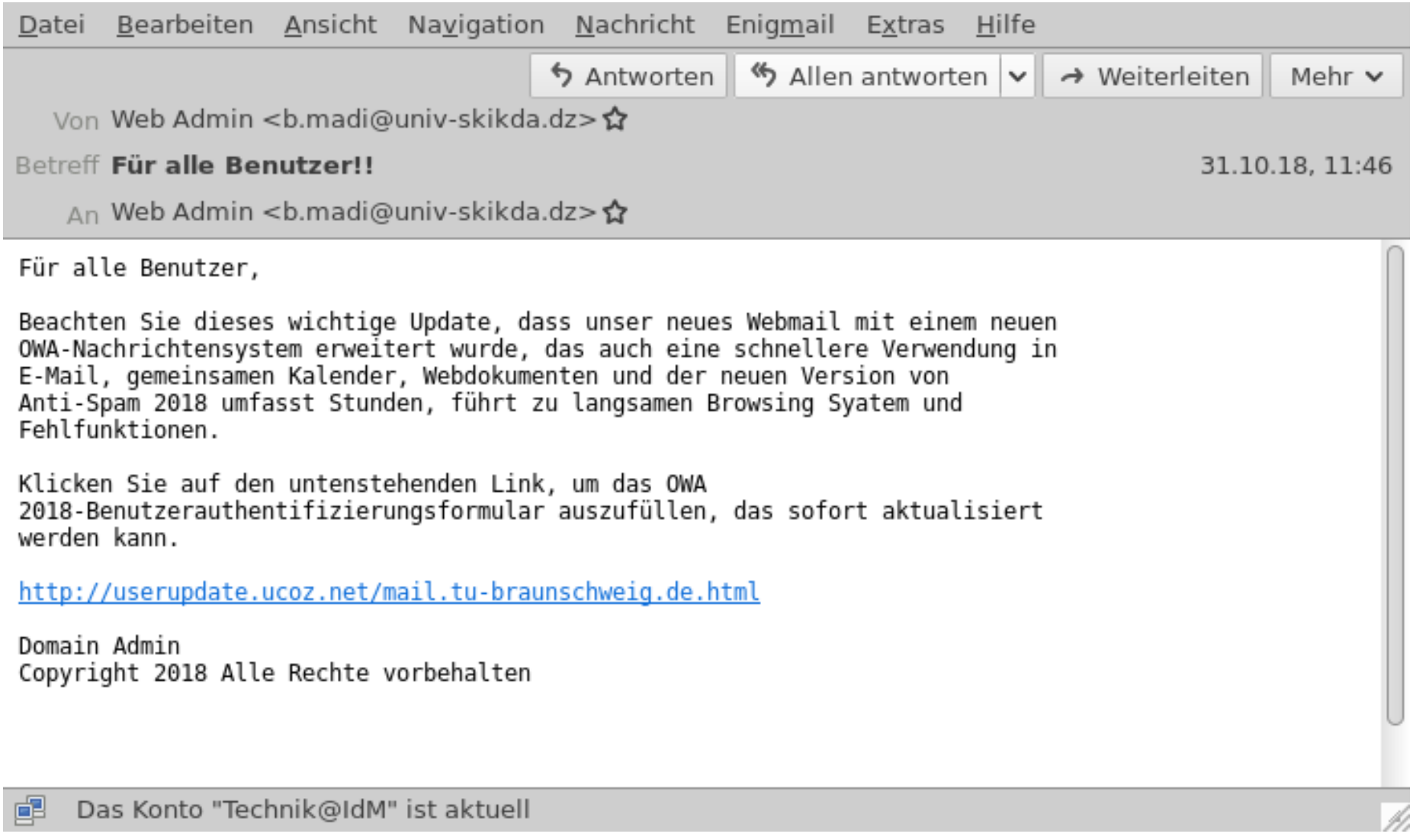
Raimund Fraatz

Mob: 0398 3 341435
Telefax: 0398 3 341626
e-Mail:Raimund.Fraatz@zuv.uni-hannover.de
-

1 Anhang: RG-LCB-9627-88508.doc 76,9 KB | Speichern



Verschlüsselung im Anhang umgeht Mail-Filterung



in HTML-Ansicht eigentliche URL versteckbar

Betreff: Nachricht vom Sicherheitsdienst. Der Zugang zu Ihrem Konto erfolgt uber Dritte.
Von: <harnisch@rrzn.uni-hannover.de>
Datum: 13.01.19, 22:53
An: <harnisch@rrzn.uni-hannover.de>

Ich grüße Sie!

Ich habe schlechte Nachrichten für dich.
28.06.2018 - an diesem Tag habe ich Ihr Betriebssystem gehackt und vollen Zugriff auf Ihr Konto erhalten harnisch@rrzn.uni-hannover.de.

Wie war es:
In der Software des Routers, mit der Sie an diesem Tag verbunden waren, gab es eine Sicherheitsanfälligkeit.
Ich habe diesen Router zuerst gehackt und meinen bösartigen Code darauf abgelegt.
Bei der Eingabe im Internet wurde mein Trojaner auf dem Betriebssystem Ihres Geräts installiert.

Danach habe ich alle Daten auf Ihrer Festplatte gespeichert (ich habe Ihr gesamtes Adressbuch, den Verlauf der angezeigten Websites, alle Dateien, Telefonnummern und Adressen aller Ihrer Kontakte).

Ich wollte dein Gerät sperren. Und benötigen Sie eine kleine Menge Geld für das Entsperren.

13.1.=Sonntag (WE / Feiertag / Ferien / nachts eher kein Admin-Eingriff)

Absender=Empfänger plausibilisiert Hack-Behauptung

Aber ich habe mir die Websites angesehen, die Sie regelmäßig besuchen, und kam zu dem großen Schock Ihrer Lieblingsressourcen.
Ich spreche von Websites für Erwachsene.

Ich möchte sagen - du bist ein großer Perverser. Sie haben ungezügelte Fantasie!

Danach kam mir eine Idee in den Sinn.
Ich habe einen Screenshot der intimen Website gemacht, auf der Sie Spaß haben (Sie wissen, worum es geht, oder?).
Danach nahm ich Ihre Freuden ab (mit der Kamera Ihres Geräts). Es stellte sich wunderbar heraus, zögern Sie nicht.

Ich bin fest davon überzeugt, dass Sie diese Bilder Ihren Verwandten, Freunden oder Kollegen nicht zeigen möchten.
Ich denke, 309€ sind ein sehr kleiner Betrag für mein Schweigen.
Außerdem habe ich viel Zeit mit dir verbracht!

Ich akzeptiere nur Bitcoins.
Meine BTC-Geldbörse: 18Pt4B7Rz7Wf491FGQHPsfDeKRqnkyrMo6

Sie wissen nicht, wie Sie die Bitcoins senden sollen?
Schreiben Sie in einer Suchmaschine "wie Sie Geld an die BTC-Geldbörse senden".
Es ist einfacher als Geld an eine Kreditkarte zu senden!

Für die Bezahlung gebe ich Ihnen etwas mehr als zwei Tage (genau 50 Stunden).
Keine Sorge, der Timer startet in dem Moment, in dem Sie diesen Brief öffnen.
Ja, ja .. es hat schon angefangen!

Nach Zahlungseingang zerstören sich meine Viren und schmutzigen Fotos automatisch.
Wenn ich die angegebene Menge nicht von Ihnen erhalte, wird Ihr Gerät gesperrt, und alle Ihre Kontakte erhalten ein Foto mit Ihren "Freuden".

Ich möchte, dass du umsichtig bist.
- Versuchen Sie nicht, mein Virus zu finden und zu zerstören! (Alle Ihre Daten sind bereits auf einen Remote-Server hochgeladen.)
- Versuchen Sie nicht, mich zu kontaktieren (Dies ist nicht möglich, ich habe Ihnen diese E-Mail von Ihrem Konto aus gesendet).
- Verschiedene Sicherheitsdienste helfen Ihnen nicht weiter; Auch das Formatieren einer Festplatte oder das Zerstören eines Geräts ist nicht hilfreich, da sich Ihre Daten bereits auf einem Remote-Server befinden.

P.S. Ich garantiere Ihnen, dass ich Sie nach der Bezahlung nicht mehr stören werde, da Sie nicht mein einziges Opfer sind.
Dies ist ein Hacker-Ehrenkodex.

Ich empfehle Ihnen von nun an, gute Antiviren-Programme zu verwenden und regelmäßig (mehrmals täglich) zu aktualisieren!

Sei nicht böse auf mich, jeder hat seine eigene Arbeit.
Abschied.

Von: Robert Miller <robert.miller@education1.teaching-research-group.com>
Gesendet: Dienstag, 15. Januar 2019 06:33
An: XYZXYZ <XYZ.XYZ@XYZ.uni-hannover.de>
Betreff: Kontaktanfrage für die Fakultätsbewerbung

Hallo, ich heiße Robert Miller. Ich bin Professor und möchte mich gerne bei Ihnen bewerben. Bitte teilen Sie mir die E-Mail-Adresse Ihres Personalverantwortlichen sowie die des akademischen Direktors, der für die Einstellung von Fakultäten zuständig ist mit. Vielen Dank im Voraus für Ihre Hilfe. Mit freundlichen Grüßen Robert Miller

Mail ist selbst völlig harmlos, sinnvoll für

- Prüfung der Empfänger-Adresse
- Kontaktanbahnung
- Empfänger als Referenz in Spear-Phishing-Mail verwenden

Vorfälle: malicious Spam / Phishing

Phishing-Beispiel

Beispiele bösartiger Mails:

- Rechnungstellung oder Bewerbung mit .doc-Anhang
- IT-Support bittet um Passwort-Änderung mit URL oder Anhang
- Erpressung: Fotos bei Pornografiekonsum
- Überweisung (CEO-Fraud)
  z.B. im LUIS Rupp an Jabben
- Spear-Phishing: Projektpartner schickt Mail mit Link zu Dokument mit Referenz auf gemeinsames Projekt
  z.B. zu echtem Projekt mit Staatskanzlei, Link zu Cloud
- Spear-Phishing: Anbahnung, über Bande (Referenz sorgt für Vertrauen)

Vorfälle: malicious Spam / Phishing

Technische Maßnahmen

- Aktivieren der Spam-Abwehr

  ⟶ auch für private Accounts

- Training der Spam-Abwehr, vgl.
  `https://www.luis.uni-hannover.de/email_spamabwehr.html`
- Unterdrückung bösartiger Anhänge (Dokumente mit Makros etc.)

  ⟶ nicht zentral machbar für andere Mail-Provider
- keine externen Inhalte anzeigen, HTML-Mails vermeiden
- URLs im DNS umlenken, URL Hoster / CERT melden (LUIS)

… und sonst das Übliche:
Endpoint-Security („Anti-Virus"), Systeme aktuell halten, Systeme restriktiv konfigurieren (Makro-Start, Admin-Rechte etc.)

Vorfälle: malicious Spam / Phishing

Zusammenfassung

- Spam ist überwiegend bösartig
- malicious Spam nimmt zu
- wenig technische Möglichkeiten
- der Mensch ist die Schwachstelle

Vorfälle: malicious Spam / Phishing

Nutzer-Aufklärung

BSI:

„Erst denken,
dann klicken.“

Problem:

Zunehmend Phishing mit 3 x „Ja.“

⇝ Awareness schwierig, alte Hinweise ggf. kontraproduktiv

Vorfälle: malicious Spam / Phishing

False Positive bei Rückmeldung Studierender

alt: Leporello enthielt Hinweis auf Rückmeldung für kommendes Semester (Frist, Betrag, Kontoverbindung)

neu: LeibnizCard macht Leporello hinfällig, daher Mail bzgl. Rückmeldung (dadurch zeitnahe Erinnerung)

zuerst: Mail mit allen Infos inkl. Kontoverbindung

$\Longrightarrow$ klingt nach Phishing, ermöglicht Phishing

danach: Mail reduziert und abgesichert

- nur Hinweis auf Rückmeldung und Frist
- URL mit Uni-Link für mehr Infos
- Hinweis auf nötiges TLS & kritische Prüfung
- digital signiert 

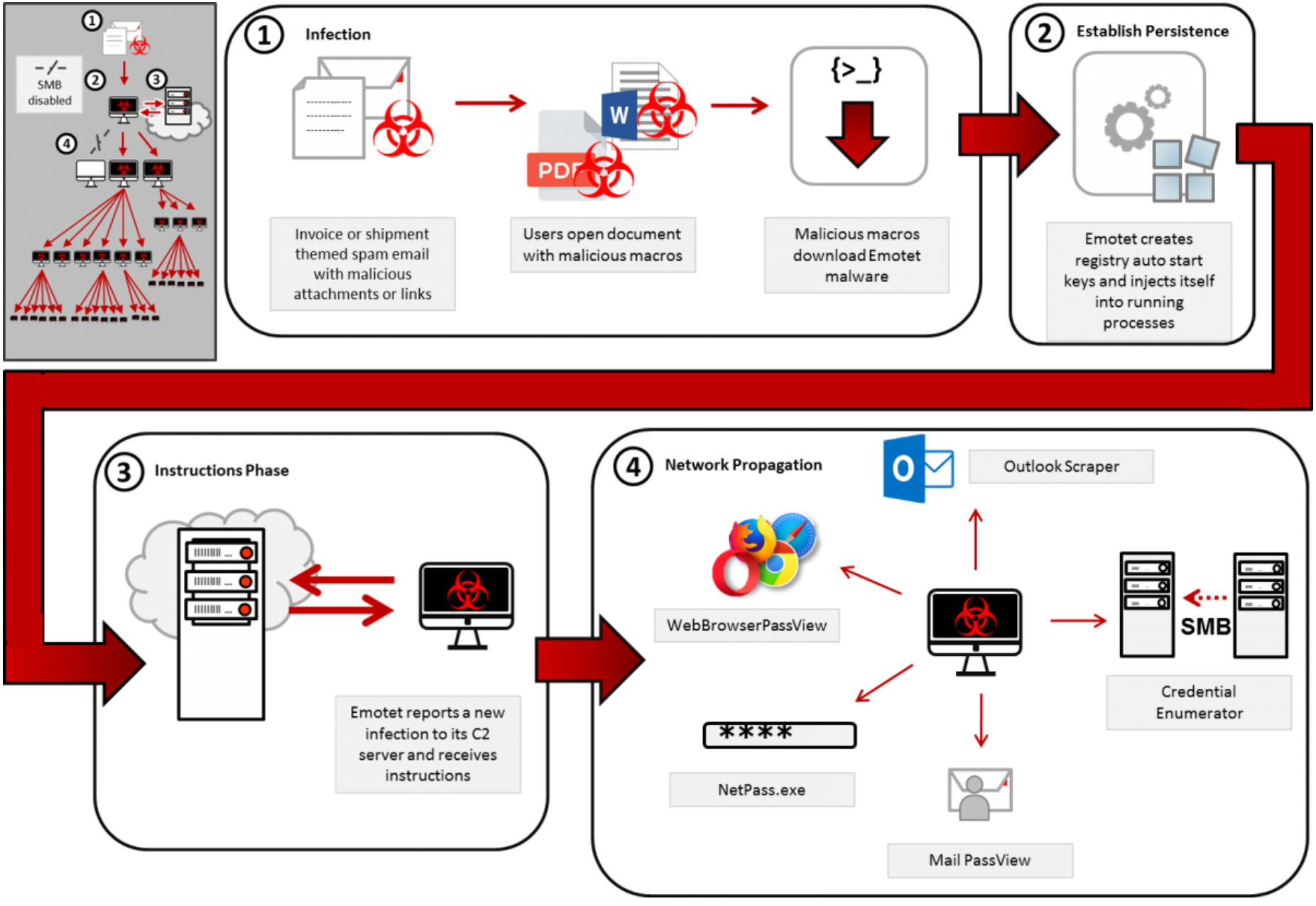
$\Longrightarrow$ Phishing bleibt natürlich nicht ausgeschlossen

Vorfälle: Emotet

Emotet als advanced malware

„Emotet continues to be among the most costly and destructive malware affecting [...] governments, and the private and public sectors." (US-Cert 7/2018)

- aktiv seit 2014, hauptsächlich Banking-Trojaner, entwickelt sich seitdem weiter
- setzt sich mehrfach im System fest (für Persistenz)
- Bot mit Credential-Abgriff und C&C-Server-Kontakt (Payload)
- verschiedene Infektionswege: Mail-Anhang, URL / Website, SMB
- mutiert, um AV-Erkennung mit Hashes zu entgehen
- erkennt virtuelle Maschinen: dann still, entzieht sich Analyse



https://www.us-cert.gov/ncas/alerts/TA18-201A

Vorfälle: Emotet

Wurmverhalten

(4) in vorangehender Grafik zeigt Weiterverbreitung:

MailPass Zugangdaten zu Mail-Accounts aus Mail-Clients

NetPass gespeicherte Netzzugangsdaten des Nutzers,
auch aus Windows-Credential-Stores auf externen Medien

Browser in Browser gespeicherte Zugangsdaten

CredEnum nutzen der Zugangdaten + Bruteforce für verfügbare
SMB-Zugänge und lokalen Admin sowie ungepatchte SMB-Lücke
für Verbreitung über Dateiinfektion

Outlook Phishing-Mails an Adressbucheinträge von Mail-Accounts

Vorfälle: Emotet

seit Q3/2018 massives Phishing

Emotet nimmt nicht nur Adressbuch mit Absender des Nutzers sondern

- analysiert Kommunikationsbeziehungen
- analysiert Mail-Inhalte
- adaptiert übliche Mail-Kommunikation des Nutzers
  wer mit wem, Anreden & Signatures, Mail-Inhalte

Art der Verbreitung + Güte des Bots

$\Longrightarrow$ Spear-Phishing & APT — automatisch, nicht handverlesen:

=: Dynamite-Phishing

Warnungen und massive Infektionsreports von allen Seiten (BSI, CERTs, BKA etc.)

Vorfälle: Emotet

Gegenmaßnahmen

- Begrenzung der SMB-Zugriffsmöglichkeiten
  - Begrenzung SMB-Traffic: existierende SMB-Sperre am Router, aber auch zwischen Clients (Windows-FW, unvertraueneswürdiges LAN)
  - restriktive Rechtevergabe auf den Shares: *principal of least privilege*
- Endpoint-Security & Patchen
- Spam- und Virenabwehr bei Mail, z.B. keine `.doc` mit Makros
- Awareness auch für Endnutzer
- *be prepared:*
  - Backup, automatisierte Neuinstallation vorsehen
  - stilllegen infizierter Systeme, ändern aller Passwörter

Vorfälle: Veranstaltungsmanagement

SW-System

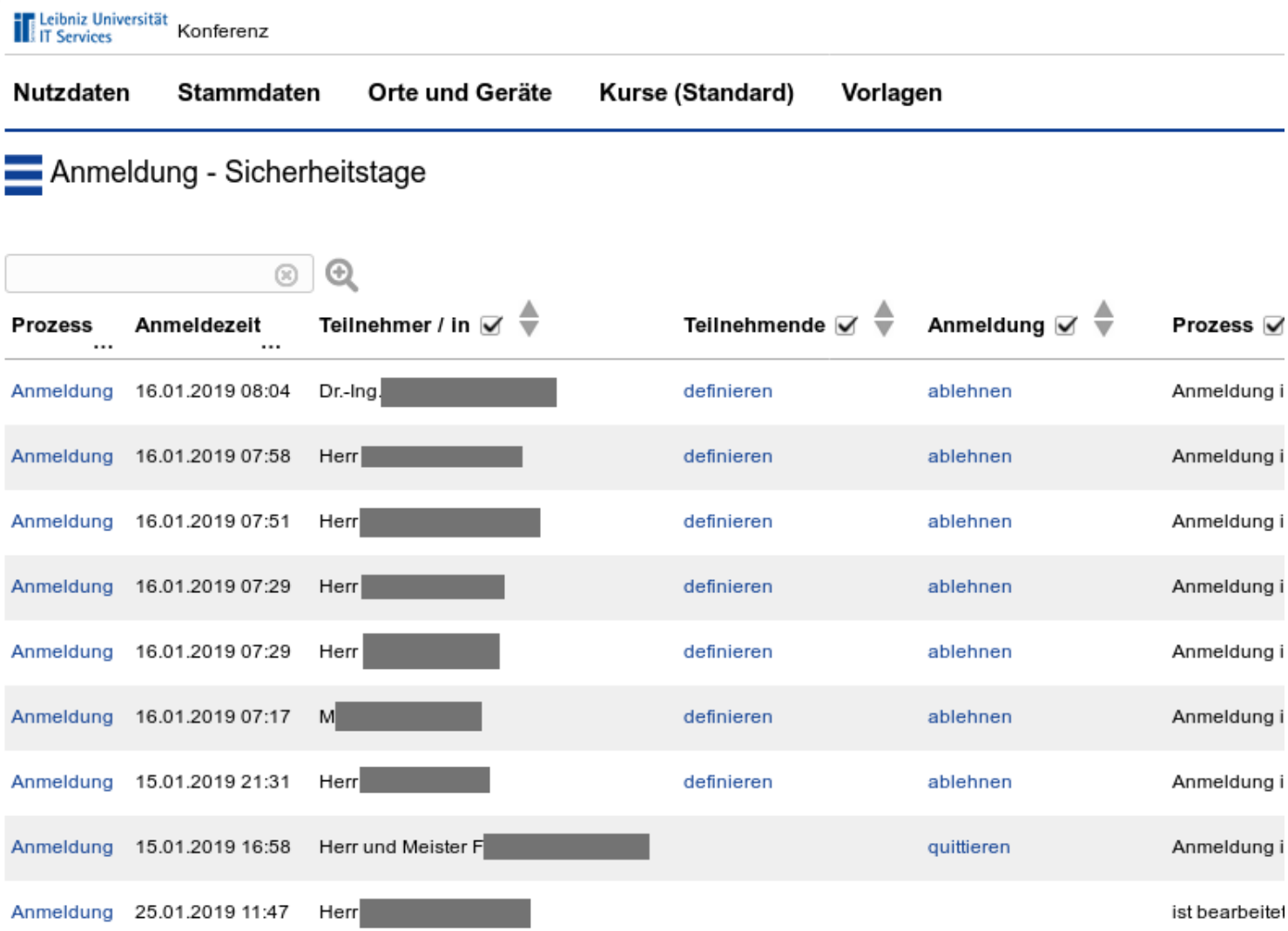
Webanwendung mit Datenbank, Front- & Backend über Web

- Grundsystem zur Abbildung von Formularen & Workflows
- angepasst zur Kurs- & Veranstaltungsverwaltung mit
  - Online-Anmeldung über Formular mit Mail-Bestätigung
  - Webschnittstelle zur Verwaltung
  - Zulassung, Teilnehmerlisten etc.
- für Anmeldung zu den Sicherheitstagen genutzt

Erste Problemmeldung war Teilnehmereinsicht, ließ sich durch Berechtigungskorrektur beheben.

Vorfälle: Veranstaltungsmanagement

auffälliges „und Meister“ …



Leibniz Universität IT Services Konferenz

Nutzdaten | Stammdaten | Orte und Geräte | Kurse (Standard) | Vorlagen

Anmeldung - Sicherheitstage

Prozess	Anmeldezeit	Teilnehmer / in	Teilnehmende	Anmeldung	Prozess
Anmeldung	16.01.2019 08:04	Dr.-Ing. [redacted]	definieren	ablehnen	Anmeldung i
Anmeldung	16.01.2019 07:58	Herr [redacted]	definieren	ablehnen	Anmeldung i
Anmeldung	16.01.2019 07:51	Herr [redacted]	definieren	ablehnen	Anmeldung i
Anmeldung	16.01.2019 07:29	Herr [redacted]	definieren	ablehnen	Anmeldung i
Anmeldung	16.01.2019 07:29	Herr [redacted]	definieren	ablehnen	Anmeldung i
Anmeldung	16.01.2019 07:17	M [redacted]	definieren	ablehnen	Anmeldung i
Anmeldung	15.01.2019 21:31	Herr [redacted]	definieren	ablehnen	Anmeldung i
Anmeldung	15.01.2019 16:58	Herr und Meister F [redacted]		quittieren	Anmeldung i
Anmeldung	25.01.2019 11:47	Herr [redacted]			ist bearbeitet

Vorfälle: Veranstaltungsmanagement

… ist nicht Teil des Vornamens:

Vorfälle: Veranstaltungsmanagement

Unwirksame/fehlende Input-Validierung

- Anrede ist Auswahlbox (leer/Herr/Frau)
- Nutzer wählt bei Ausfüllen des Anmeldeformulars aus
- und schickt Formular an Server.

soll Server akzeptiert nur einen der vergeschlagenen Werte

ist Server akzeptiert auch anderes

$\Longrightarrow$ Server validiert (generell?) Input nicht (ausreichend).

- mind. Client wenn nicht auch Server selbst verarbeiten nicht-vertrauenswürdige Werte
- falls Server: SQL-Injection etc.
- falls nur Client: XSS, ggf. persistent

Vorfälle: Veranstaltungsmanagement

Handling von Session-Data

- Veranstaltungsdaten etc. werden über Hidden-Input-Felder zwischen Seiten übergeben
- Problem: Daten waren beim Client $\Rightarrow$ nicht-vertrauenswürdig

soll Daten serverseitig führen, ggf. Daten signieren

ist Daten werden ungeprüft weiterverwendet

$\Longrightarrow$ z.B. Mail-Empfänger und -Text für Anmeldebestätigung beliebig veränderbar

$\Longrightarrow$ gut verwendbar für Phishing (vertrautes Absendersystem)

Vorfälle: Veranstaltungsmanagement

Reaktion

Nach Meldung der Einsicht in Teilnehmerliste:

- Anpassung der Rechte, auch bei Inkaufnahme von Seiteneffekten (hier: leere Bestätigungsmails)

Nach Auftauchen des „Meisters“:

- Test einiger Ausnutzungen des Problems, detailliertere Einsicht
- Sperrung des Systems, manuelles Ersatzverfahren
- Unterrichtung Hersteller …

Lehren

- altbekannte Sicherheitslücken weiterhin problematisch
- eigentlich *low hanging fruits*
- kommerzielle Produkte können Anfängerfehler enthalten

Vorfälle: Data-Leakage

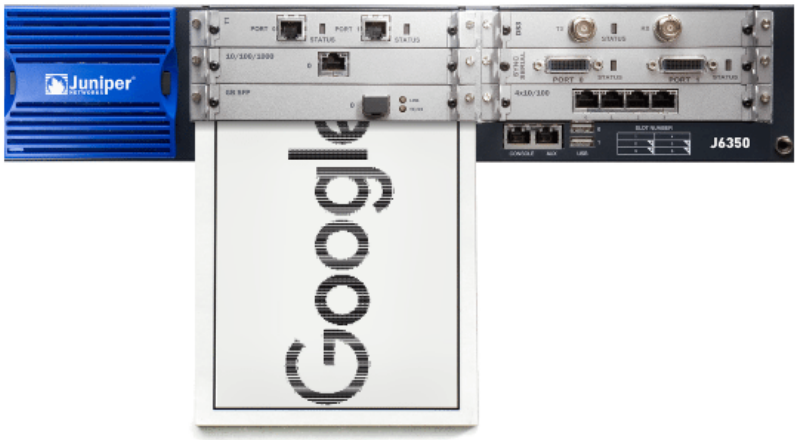
Entsorgung

heise Security News Hintergr

Security > Hintergrund > Analysiert: Google-Interna im Second-Hand-Shop

Analysiert: Google-Interna im Second-Hand-Shop

Hintergrund 06.10.2015 09:43 Uhr – Florian Heinz, Martin Kluge



Ein in Deutschland gekaufter Gebraucht-Router hatte offenbar einen prominenten Vorbesitzer. Es lieferte den neuen Besitzern interessante und brisante Einblicke in die Infrastruktur von Google – einschließlich Zugangsdaten.

INHALTSVERZEICHNIS

ähnlich LUH:

PC inkl. ungelöschter Festplatte im Müll.

Druckrolle von LeibnizCard (Thermotransfer)

Vorfälle: Data-Leakage

Datenträgerverschlüsselung

- für mobile Geräte längst Best-Practice,
  auch bereits auf Sicherheitstagen (u.a. 2009 & 2012) thematisiert
- für Notebooks mit Self-Encrypting-Disks, Bitlocker o.ä.
  vgl. https://www.luis.uni-hannover.de/its_encryption.html
- mehrere verlorene Notebooks mit unverschlüsselten Festplatten
- explizite verbindliche Regelung in Vorbereitung

Ergreifen geeigneter, üblicher Sicherheitsmaßnahmen („Stand der Technik") ist auch ohne explizite Vorgabe Pflicht.