Karl Otto Feger

„Mitarbeiter-sensibilisierung durch Phishing“

4. Kommunaler IT-Sicherheitskongress 2017

„Umsetzung der Leitlinie für Informationssicherheit des IT-Planungsrats in Kommunalverwaltungen“

STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Augen auf!

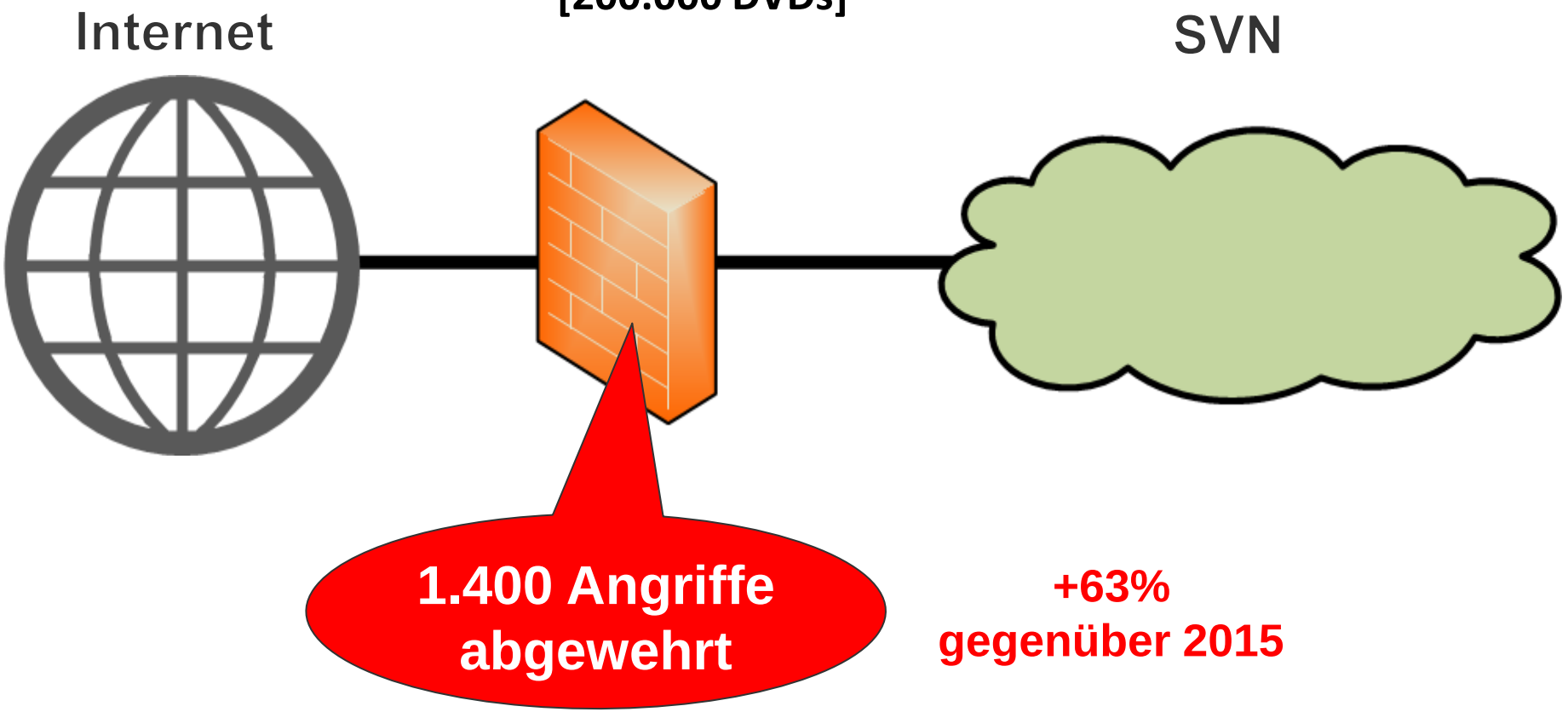
Meine Agenda für heute

- Das Angriffsziel SVN in Zahlen
- Wurden Sie heute schon gehackt?
- Warum konnten Sie eigentlich gehackt werden?
- Anatomie eines Angriffs
- Augen auf!...Ihre Rolle als Nutzer
- Schlussbetrachtungen

Das Angriffsziel SVN in Zahlen

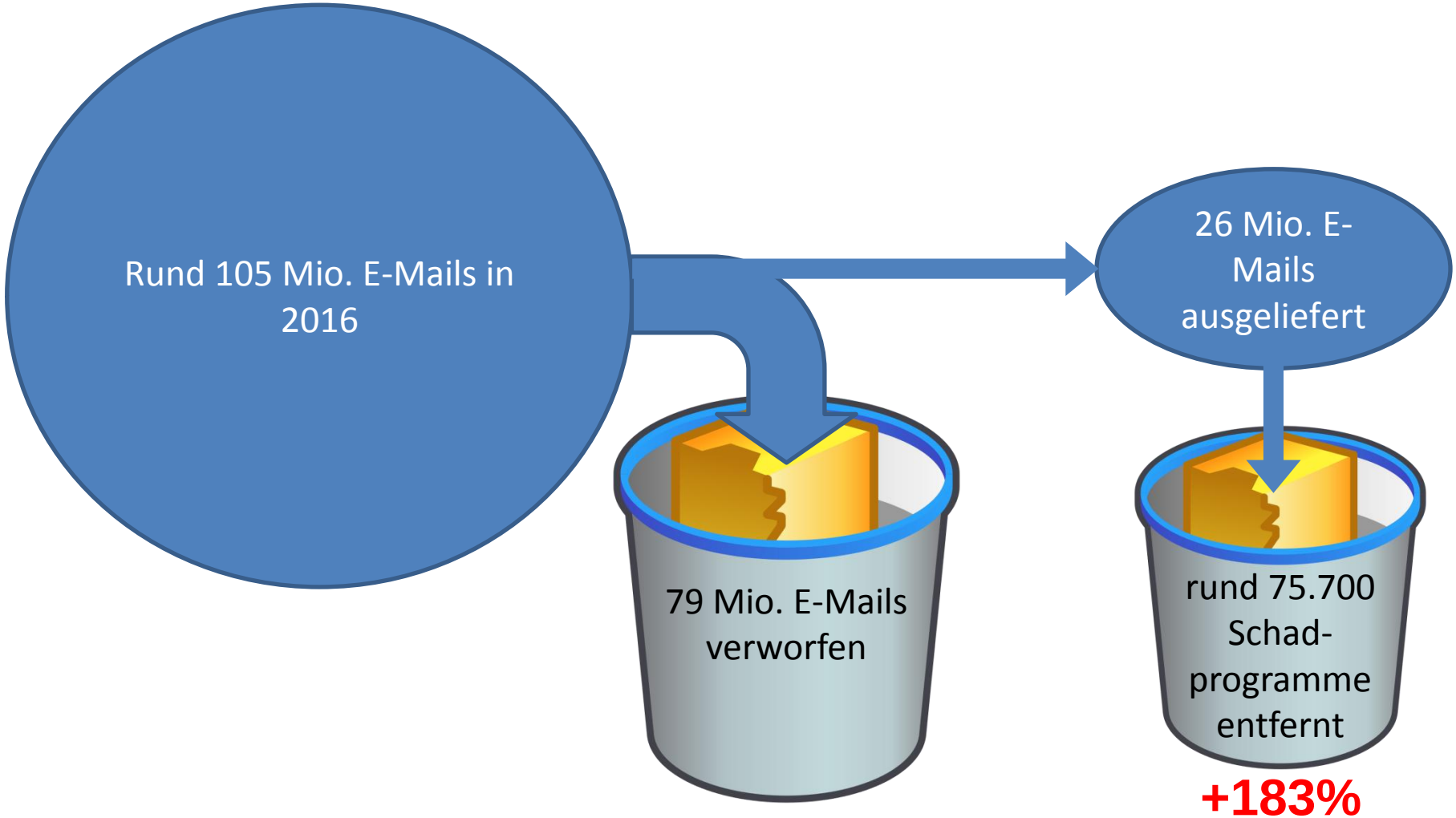
Lageübersicht SVN: Angriffe 2016

Insgesamt rund 1 Petabyte pro Jahr eingehender Verkehr im SVN
(entspricht 1.000 Terabyte bzw. 1.000.000.000.000.000 Byte)
[200.000 DVDs]



Das Angriffsziel SVN in Zahlen

Lageübersicht SVN: E-Mail 2016



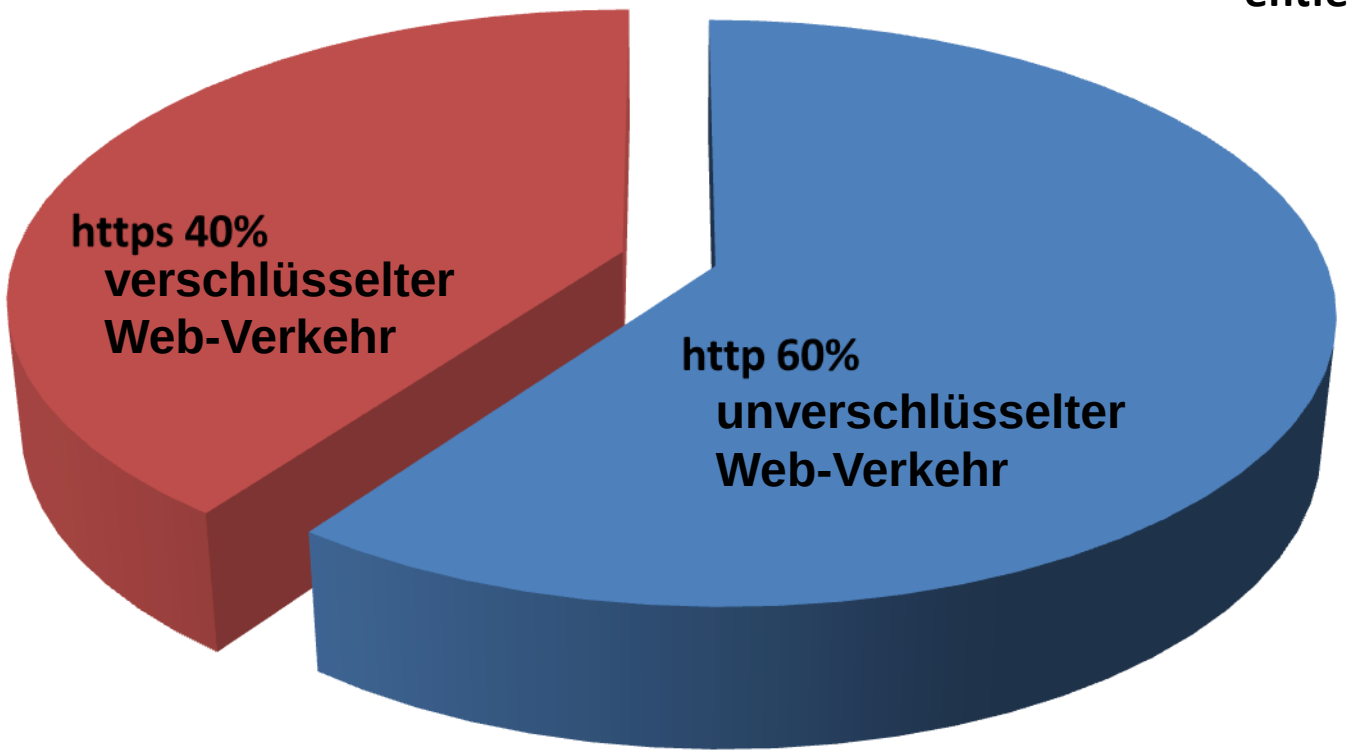
+183%
gegenüber 2015

Das Angriffsziel SVN in Zahlen

Lageübersicht SVN: Internetverkehr 2016

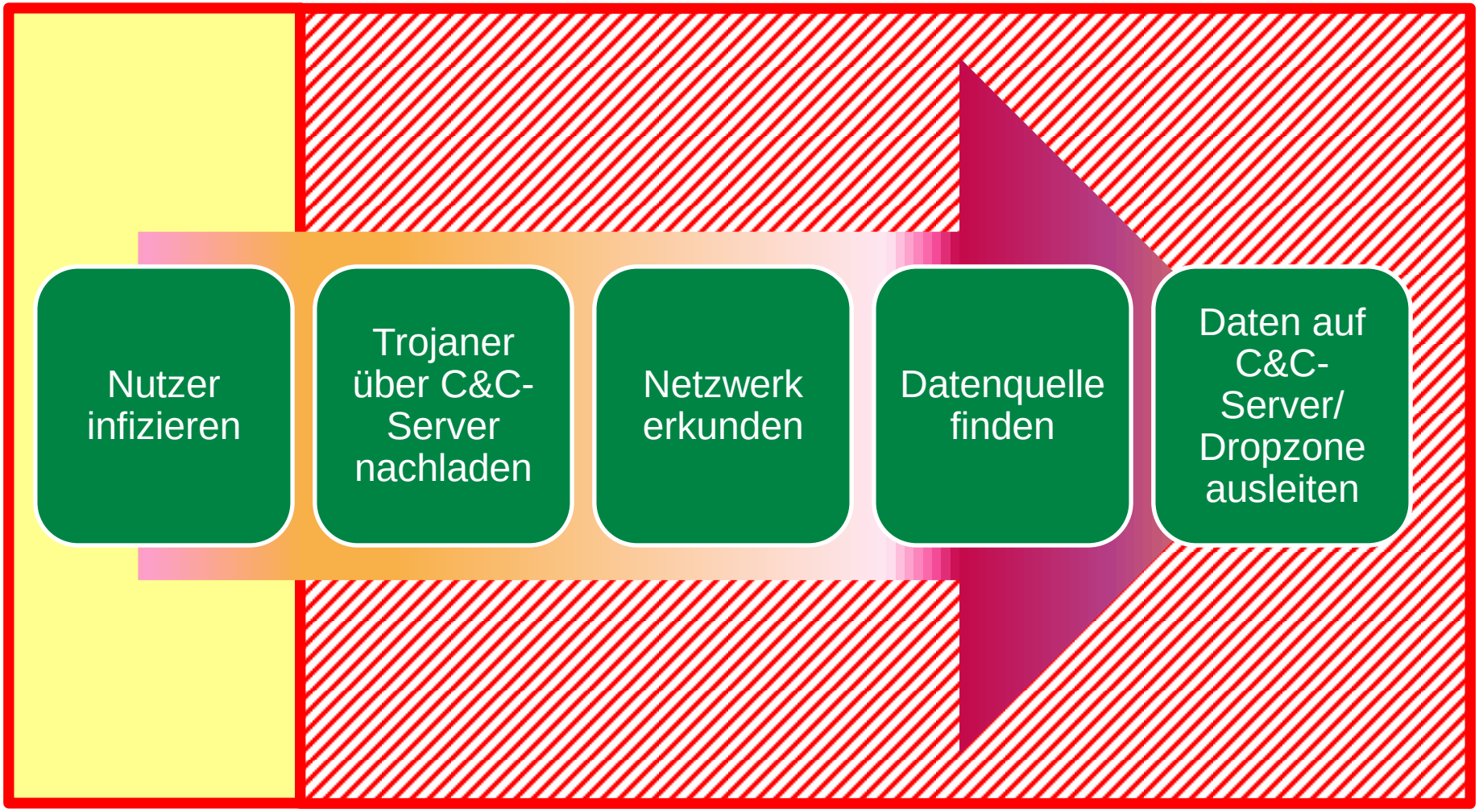
Verschlüsselter Verkehr kann (darf) nicht gescannt werden.

rund 50.000 Schadprogramme im unverschlüsseltenWeb-Verkehr entfernt



Anatomie eines Angriffs

…gebt her Eure Daten…



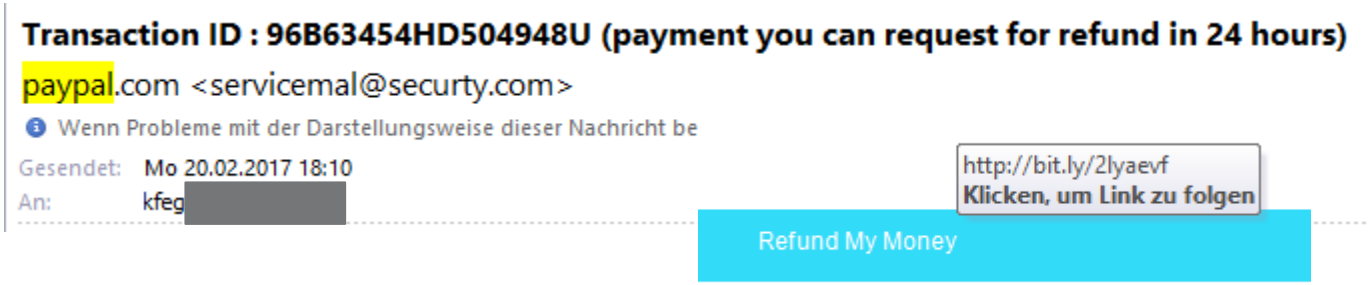
Angriffswege der Hacker

- Angriff durch Webseiten
  - Durch gehackte oder absichtlich schädliche Webseiten
  - Durch Schadsoftware in Werbung auf legitimen Webseiten
  - Durch Leichtgläubigkeit oder Leichtsinn des Besuchers (später dazu mehr)

- Angriff durch E-Mail
  - „Mit der Schrotflinte“, Phishing
    - DHL-Trojaner
  - Gezielt nach Social Engineering, Spear Phishing
    - Analyse von Facebook, Twitter,…
    - Angriff „Rolf Drescher“: BA, Stepstone, Monster,…?

Bleiben Sie aufmerksam!

Phishing



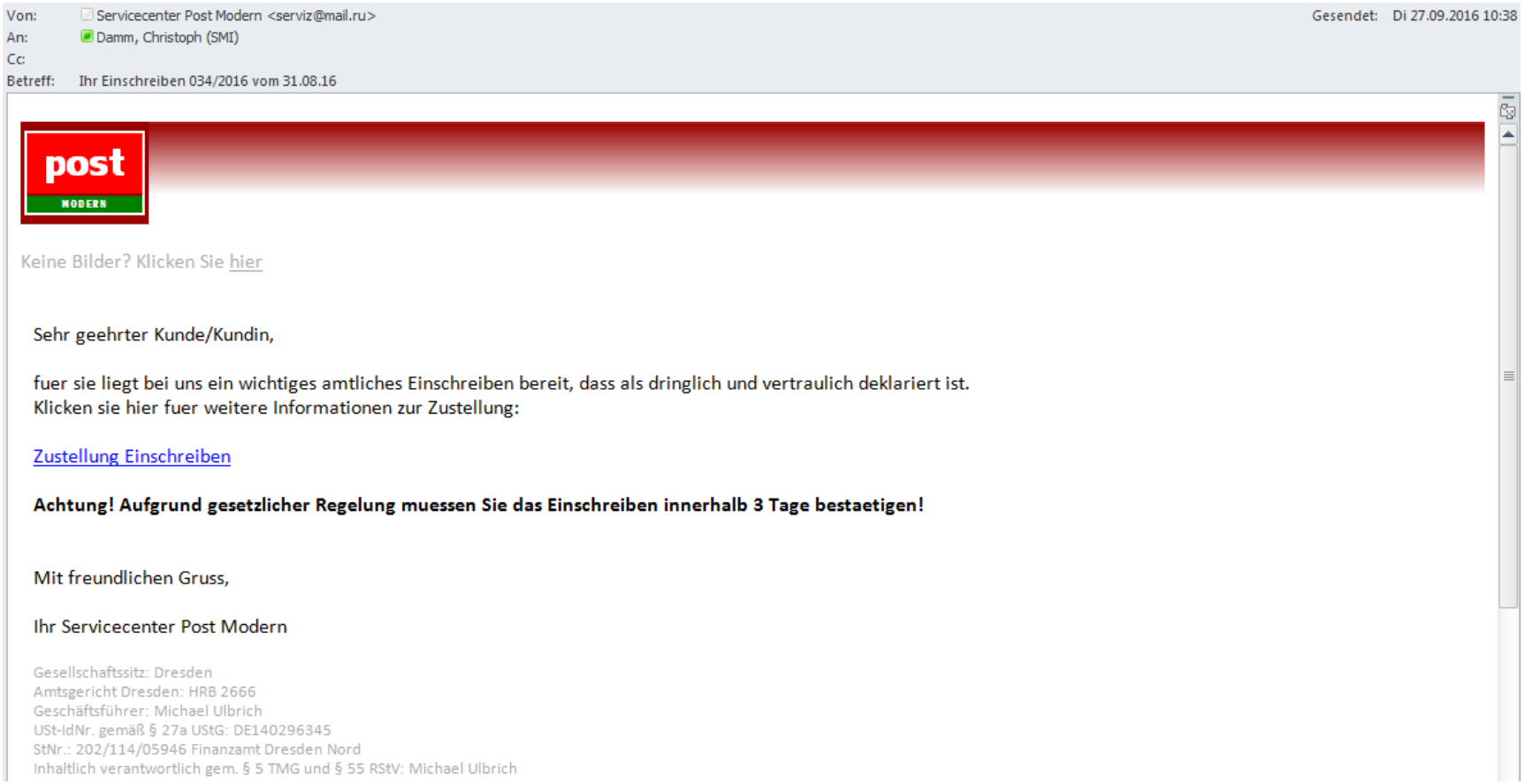
Spear Phishing

Subject: Bewerbung als er

Sehr geehrter Herr XXX, (XXX: Richtiges Geschlecht und richtiger Name eines Personal-Mitarbeiters)

hiermit bewerbe ich mich bei Ihnen für die die Stelle als er. Meine vollständigen Bewerbungsunterlagen können Sie dem Anhang entnehmen. Ich freue mich auf Ihre Rückmeldung und stehe Ihnen bei Rückfragen jederzeit gerne zur Verfügung. Mit freundlichen Grüßen Rolf Drescher

Phishingtest #1 (27. September 2016)



Von: Servicecenter Post Modern <serviz@mail.ru>
An: Damm, Christoph (SMI)
Cc:
Betreff: Ihr Einschreiben 034/2016 vom 31.08.16
Gesendet: Di 27.09.2016 10:38

post MODERN

Keine Bilder? Klicken Sie hier

Sehr geehrter Kunde/Kundin,

fuer sie liegt bei uns ein wichtiges amtliches Einschreiben bereit, dass als dringlich und vertraulich deklariert ist.
Klicken sie hier fuer weitere Informationen zur Zustellung:

Zustellung Einschreiben

Achtung! Aufgrund gesetzlicher Regelung muessen Sie das Einschreiben innerhalb 3 Tage bestaetigen!

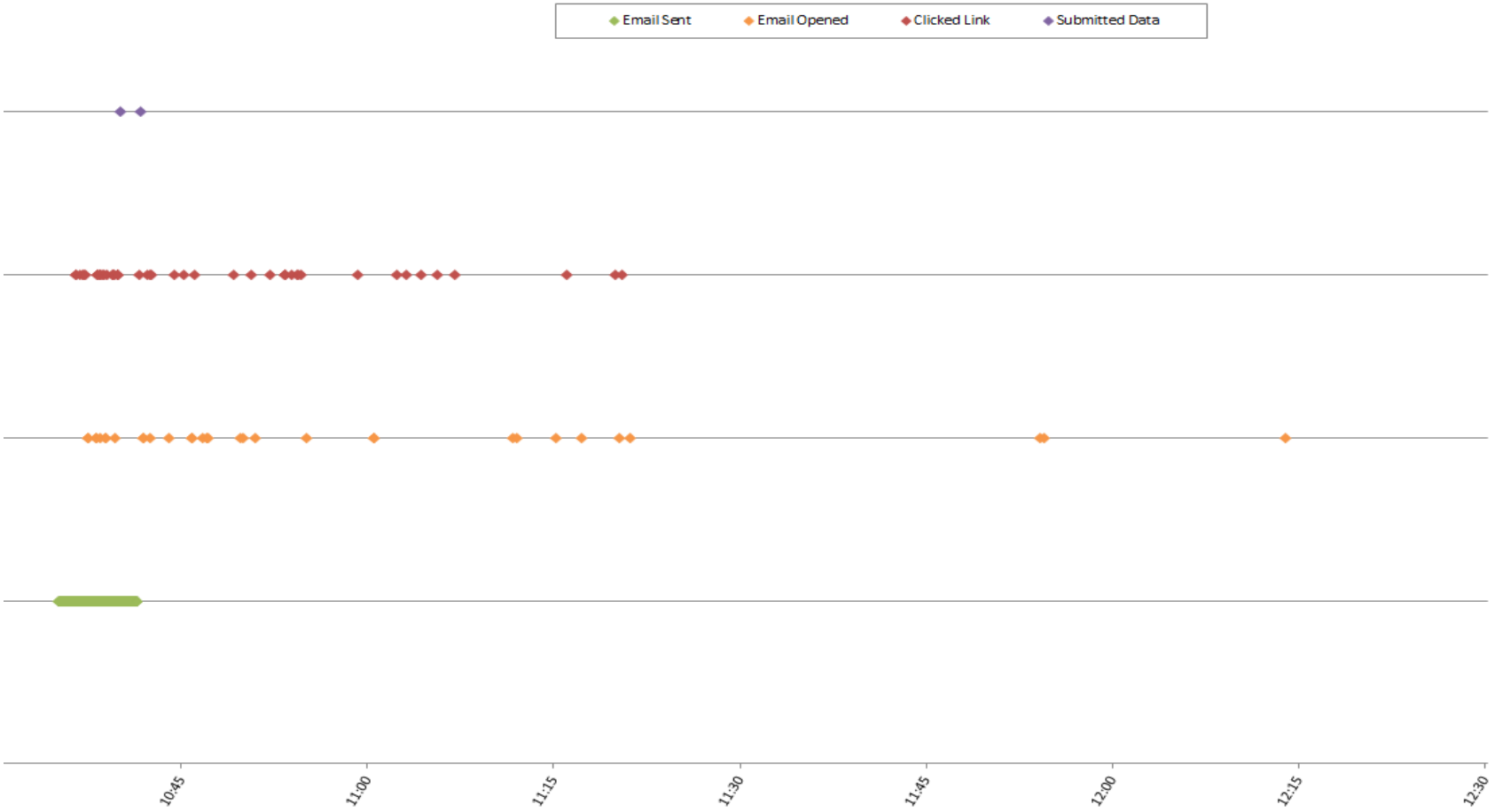
Mit freundlichen Gruss,

Ihr Servicecenter Post Modern

Gesellschaftssitz: Dresden
Amtsgericht Dresden: HRB 2666
Geschäftsführer: Michael Ulbrich
USt-IdNr. gemäß § 27a UStG: DE140296345
StNr.: 202/114/05946 Finanzamt Dresden Nord
Inhaltlich verantwortlich gem. § 5 TMG und § 55 RStV: Michael Ulbrich

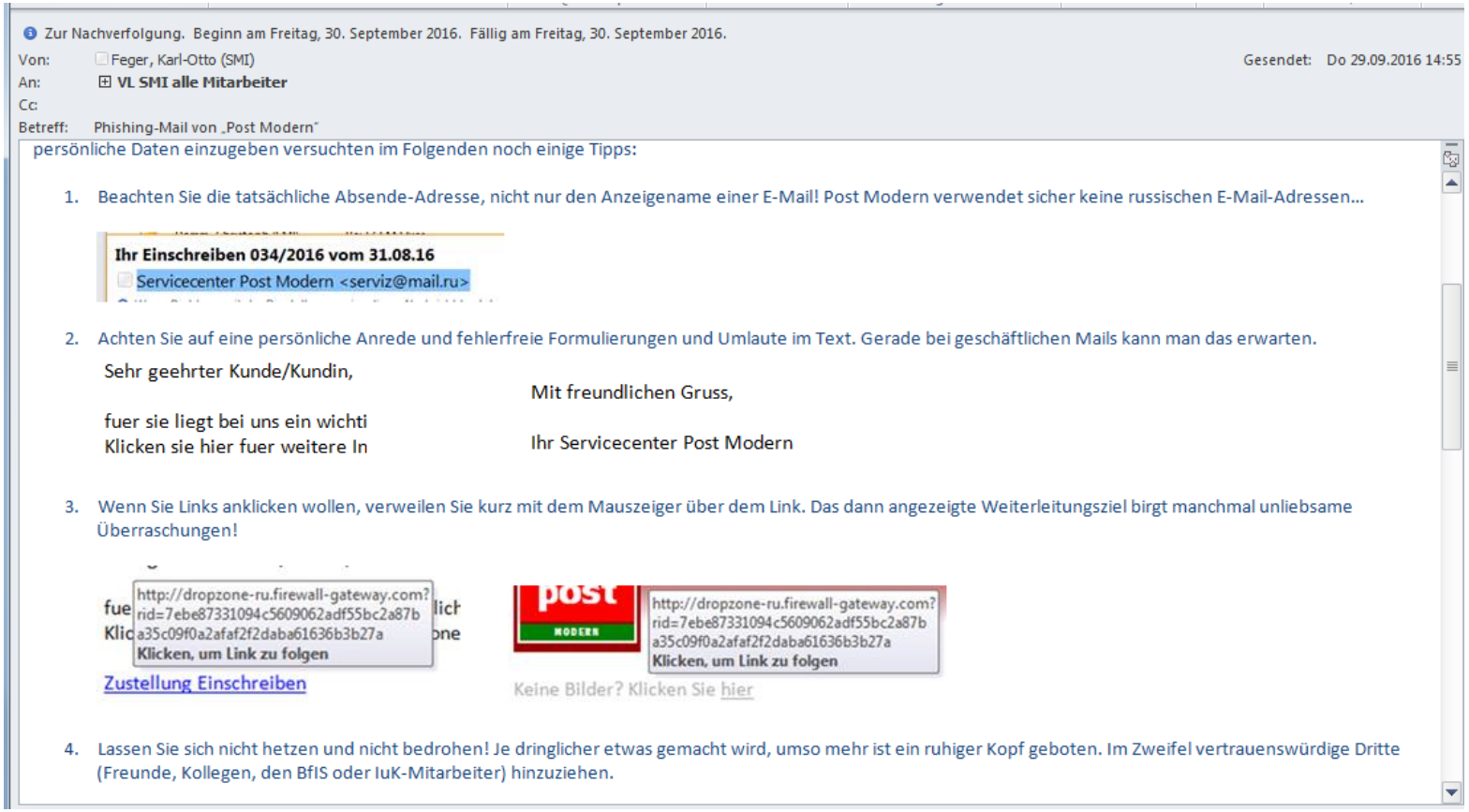
Phishingtest #1 (27. September 2016)

Ergebnisse



Phishingtest #1 (27. September 2016)

Auflösung und erneute Sensibilisierung



Zur Nachverfolgung. Beginn am Freitag, 30. September 2016. Fällig am Freitag, 30. September 2016.

Von: Feger, Karl-Otto (SMI)
Gesendet: Do 29.09.2016 14:55
An: VL SMI alle Mitarbeiter
Cc:
Betreff: Phishing-Mail von „Post Modern"

persönliche Daten einzugeben versuchten im Folgenden noch einige Tipps:

1. Beachten Sie die tatsächliche Absende-Adresse, nicht nur den Anzeigename einer E-Mail! Post Modern verwendet sicher keine russischen E-Mail-Adressen...

Ihr Einschreiben 034/2016 vom 31.08.16
Servicecenter Post Modern <serviz@mail.ru>

2. Achten Sie auf eine persönliche Anrede und fehlerfreie Formulierungen und Umlaute im Text. Gerade bei geschäftlichen Mails kann man das erwarten.

Sehr geehrter Kunde/Kundin,

fuer sie liegt bei uns ein wichti
Klicken sie hier fuer weitere In

Mit freundlichen Gruss,

Ihr Servicecenter Post Modern

3. Wenn Sie Links anklicken wollen, verweilen Sie kurz mit dem Mauszeiger über dem Link. Das dann angezeigte Weiterleitungsziel birgt manchmal unliebsame Überraschungen!

http://dropzone-ru.firewall-gateway.com?rid=7ebe87331094c5609062adf55bc2a87ba35c09f0a2afaf2f2daba61636b3b27a
Klicken, um Link zu folgen

Zustellung Einschreiben

http://dropzone-ru.firewall-gateway.com?rid=7ebe87331094c5609062adf55bc2a87ba35c09f0a2afaf2f2daba61636b3b27a
Klicken, um Link zu folgen

Keine Bilder? Klicken Sie hier

4. Lassen Sie sich nicht hetzen und nicht bedrohen! Je dringlicher etwas gemacht wird, umso mehr ist ein ruhiger Kopf geboten. Im Zweifel vertrauenswürdige Dritte (Freunde, Kollegen, den BfIS oder IuK-Mitarbeiter) hinzuziehen.

Phishingtest #2 (01. Dezember 2017)

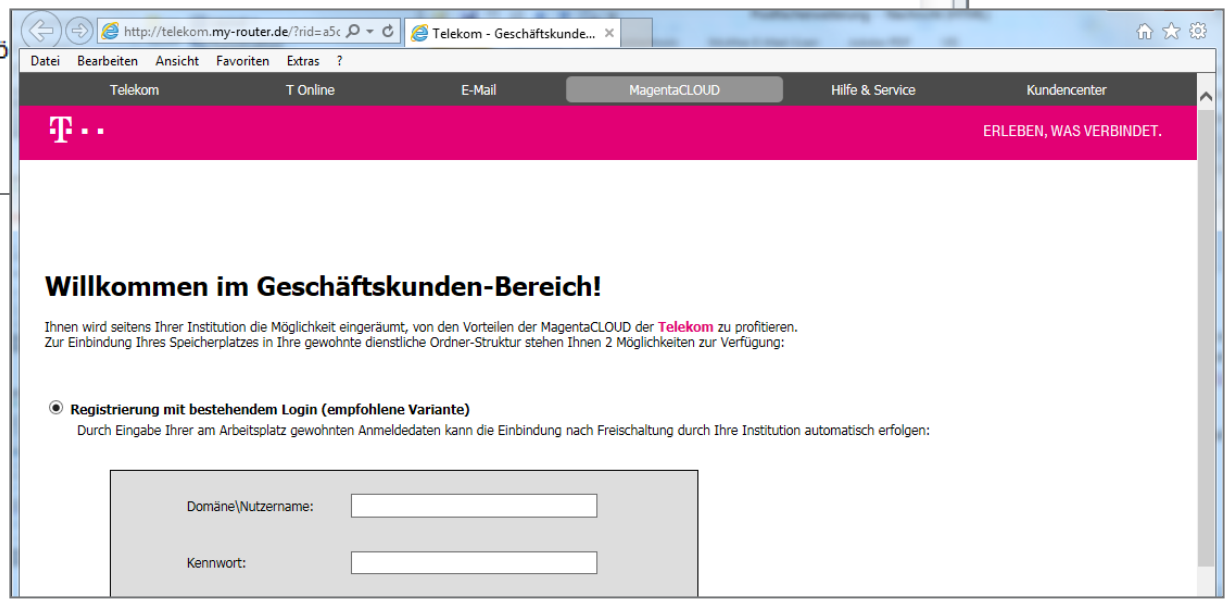
Von: IT-Service <postfacherweiterungsaktion@t-online.de> Gesendet: Do 01.12.2016 10:28
An: Damm, Christoph (SMI)
Cc:
Betreff: Postfacherweiterung

Sehr geehrt(e) KollegInnen und Kollegen,

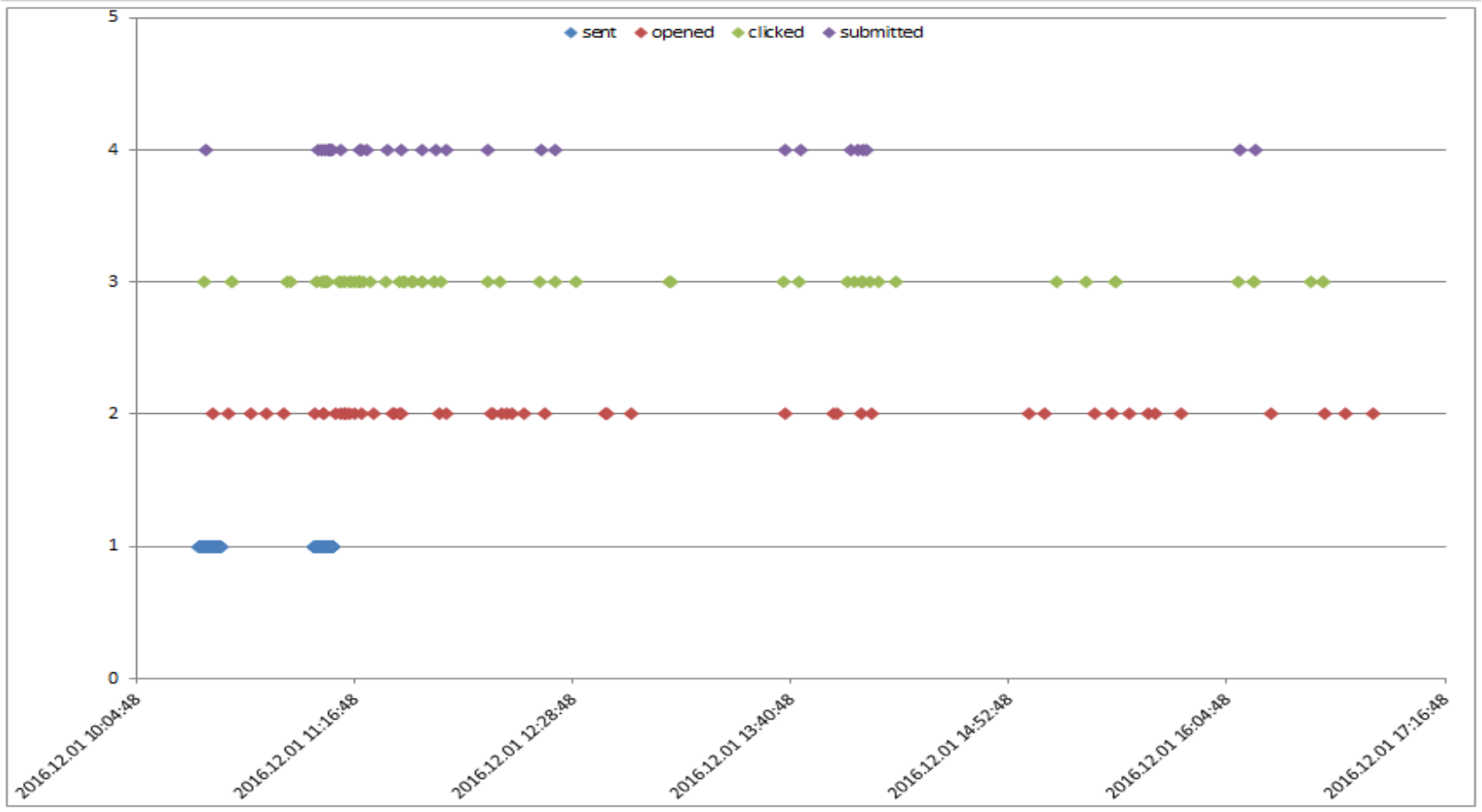
das IT-Service-Team freut sich Ihnen bezüglich ihrer IT-Ausstattung bei Bedarf eine Postfacherweiterung zusammen mit unserem Vertragspartner, der Deutschen Telekom anzubieten. Zur Erweiterung ihres dienstlichen E-Mail-Postfachs um einen dienstlich und privat nutzbaren Cloud-Speichers (5 Gigabyte) zum vereinfachten Datenaustausch folgen Sie dem Link auf die Aktionswebseite der Telekom und registrieren sie sich mit ihren gewohnten Arbeitsplatz-Anmeldedaten.

Um die Beschaffung fristgemäss durchführen zu kö

Mit freundlichen Gruß
Ihr IT-Service-Team



Phishingtest #2 (01. Dezember 2017)



Phishingtests:
Das Ergebnis heißt **mehr Sensibilisierung**

„Computernutzer, die bewusst im Internet surfen und Cybergefahren erkennen können, sind der beste Virenschutz. Daher engagiert sich die Staatsverwaltung in vielen Projekten für ein hohes Maß an Sicherheit im Cyberraum“

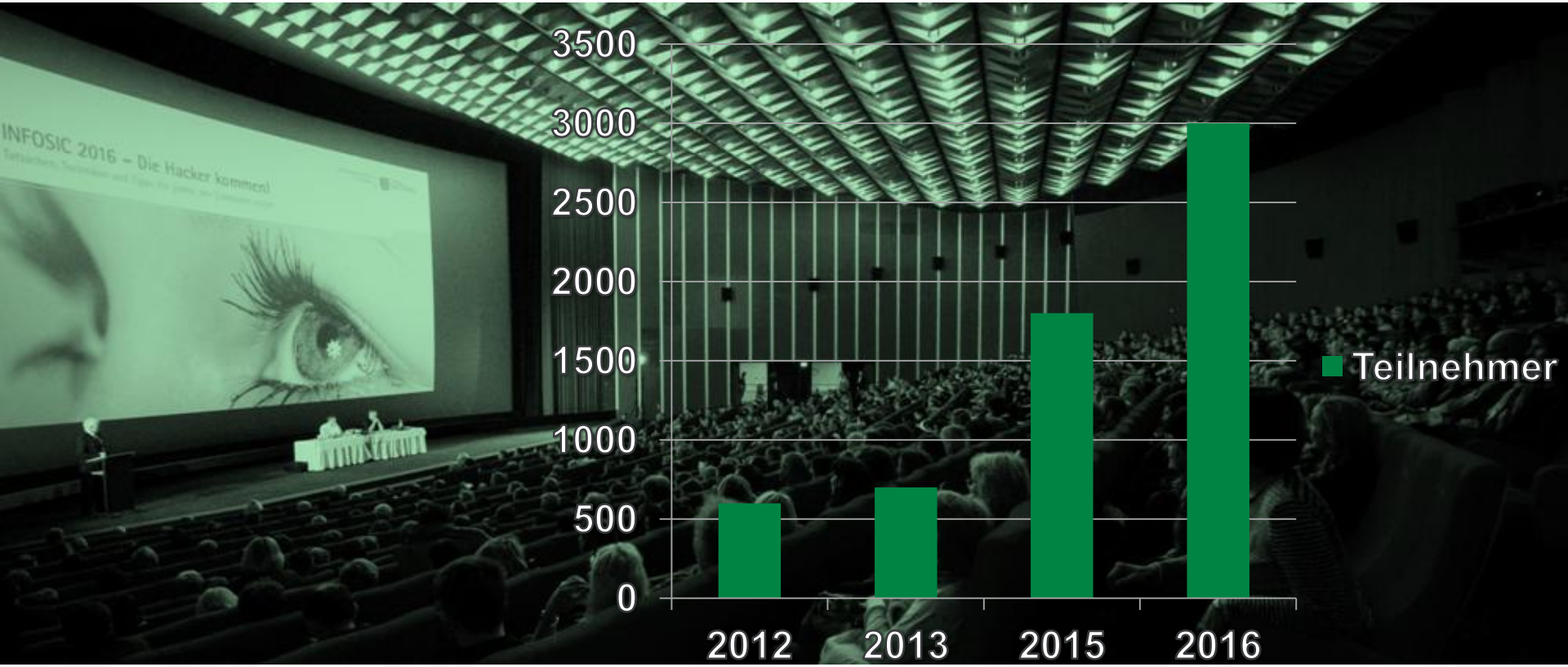
Markus Ulbig, Sächsischer Staatsminister des Innern

Sensibilisierung zur Informationssicherheit
INFOSIC

- **Die INFOSIC ist die größte Sensibilisierungs-maßnahme auf Landesebene**
- Titel: „Die Hacker kommen! – Techniken, Tipps und Tricks für jeden der Computer nutzt“
- In einer unterhaltsamen Mischung aus Vorträgen und Technikdemonstrationen („Live-Hacking“) gibt es hier leicht verständliche Informationen und Tipps zu den zentralen Themengebieten der Informationssicherheit:
  - Gefährdungen durch die Nutzung der modernen Informationstechnik
  - Tücken der Internetnutzung
  - Mobilität mit Sicherheitslücken
  - Der Mensch als Angriffsziel von Hackern

INFOSIC – eine Erfolgsgeschichte

Teilnehmerzahlen 2012-2016



Sensibilisierung zur Informationssicherheit
E-Learning

- **Präsenzveranstaltungen sind bei schätzungsweise 40.000 Computerarbeitsplätzen in der sächsischen Landesverwaltung innerhalb des SVN kein alleiniges Heilmittel – deshalb: E-Learning.**
- In Zusammenarbeit mit TU Dresden Weiterentwicklung eines bestehenden E-Learning-Angebots der BAköV
- Anpassung an die Gegebenheiten der sächsischen Landesverwaltung mit den für sie relevanten Gesetzen sowie Entwicklung eigener grafischer Oberfläche
- Anfang 2017 Beta-Test durch rund 100 Mitarbeiter der Verwaltung
- Aktuell: Einarbeitung der Hinweise und Vorbereitung des landesweiten Betriebs
- Und @gar hilft uns dabei!

Schlussbetrachtung

- Im Kampf um die Sicherheit unserer Netze und Systeme stehen sich Angreifer mit viel Zeit und Energie und Verteidiger mit geringer Reaktionszeit gegenüber.
  - Es tobt der Kampf „Gehirn gegen Gehirn“
- Technische Lösungen.
  - Die technische Aufrüstung des SVN und des SMI im Speziellen in Arbeit
  - Die technische Sperrung von Onlinespeicherdiensten, Webmailern und Werbenetzwerken für das SMI ist seit 01. März 2017 aktiv.
- **Sensibilisierung der Mitarbeiter**.
  - Die INFOSIC wird fortgesetzt.
  - E-Learning wird ab Q3/2017 landesweit angeboten.
    - Zusammen mit dem Sächsischen Informationssicherheits-Schein!

Danke für die Aufmerksamkeit!
Fragen?

Karl-Otto Feger
Referatsleiter 65
BfIS Land
Sächsisches Staatsministerium des Innern
karl-otto.feger@smi.sachsen