Einfallstor Phishing Mails – Hacker gehen den Weg des geringsten Wiederstands

Murat Isik
Sales Engineer

SOPHOS EVOLVE

Sophos – mehr als 30 Jahre Erfahrung

1985
GRÜNDUNG
OXFORD, UK

630M
UMSATZ
(FY17)

3.000
MITARBEITER

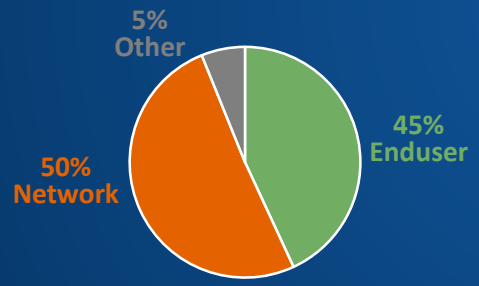
400
in DACH

HQ
ABINGDON, UK

200,000+
KUNDEN

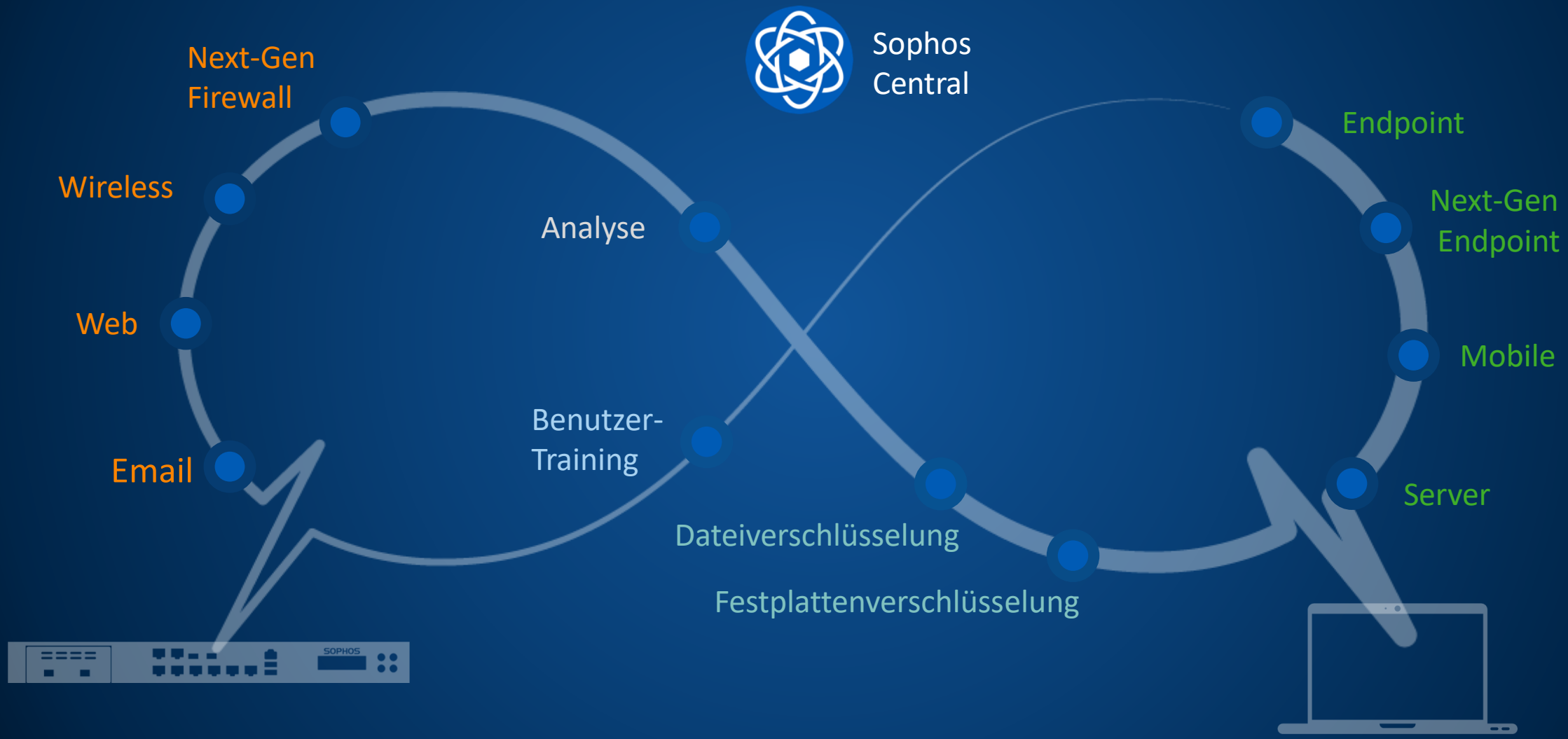
100M+
ANWENDER

20,000+
CHANNEL
PARTNER



- Akquisition u.a. von Utimaco 2009, Astaro 2011, Dialogs 2012, Cyberoam 2014, Mojave 2014, Reflexion 2015, SurfRight 2015, Barricade 2016, Invincea 2017
- Gartner: Marktführer in den Bereichen Endpoint, Verschlüsselung & UTM

Synchronized Security – Teamplay statt Best-of-Breed



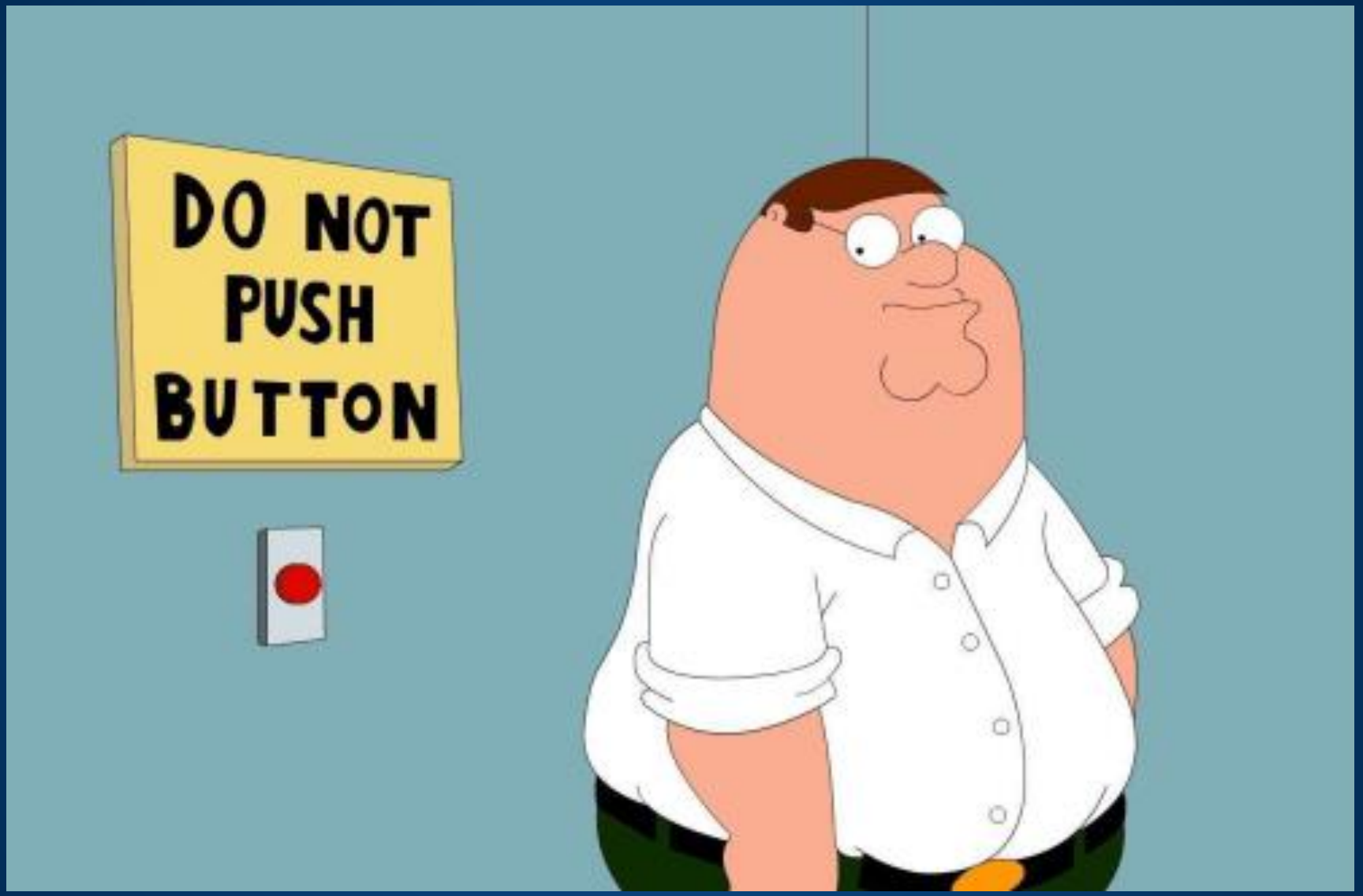
Umfrage zur IT-Sicherheit: Mitarbeiter sind Schwachstelle

30.07.2018 07:47 Uhr

vorlesen

(Bild: dpa, Monika Skolimowska/Illustration)

Das größte Risiko sitzt vor dem Rechner, sagen Sicherheitsexperten in einer Umfrage mehrheitlich. Das Problem werde von vielen Unternehmen vernachlässigt.


DO NOT
PUSH
BUTTON

Es war einmal..

Heute..

Phish

From: TV Licensing
To:
Cc:
Subject: Pay for your TV licence
Sent: Tue 3/7/2017 10:18

You're now covered to enjoy your favourite programmes.

TV LICENSING
tvlicensing.co.uk

Dear Customer,
Pay for your TV Licence.

TV Licensing informs you of the need to buy a TV Licence

You need to be covered by a TV Licence to watch or record live TV programmes on any channel, or to download or watch any BBC programmes on iPlayer – live, catch up or on demand.

This applies to any device and provider you use, including a TV, desktop computer, laptop, mobile phone, tablet, games console, digital box or DVD/Blu-ray/VHS recorder.

View Invoice

Your TV Licence details:	
Licence number:	
Licence expiry date:	09 March 2017

In the UK
we spend almost 24 hours
a week watching TV

Echt

From: TV Licensing
To:
Cc:
Subject: Thanks for buying your TV Licence
Sent: Fri 2/24/2017 10:07

You're now covered to enjoy your favourite programmes.

TV LICENSING
tvlicensing.co.uk

Dear Mrs ,
Thanks for buying your TV Licence.

You're now covered up to the end of February 2018.

Please keep this email safe, as it tells you how to update your licence details. If you ever need to change anything, just sign in to your licence. Then you can:

- update your contact details,
- tell us you've moved home, or
- print or download your licence.

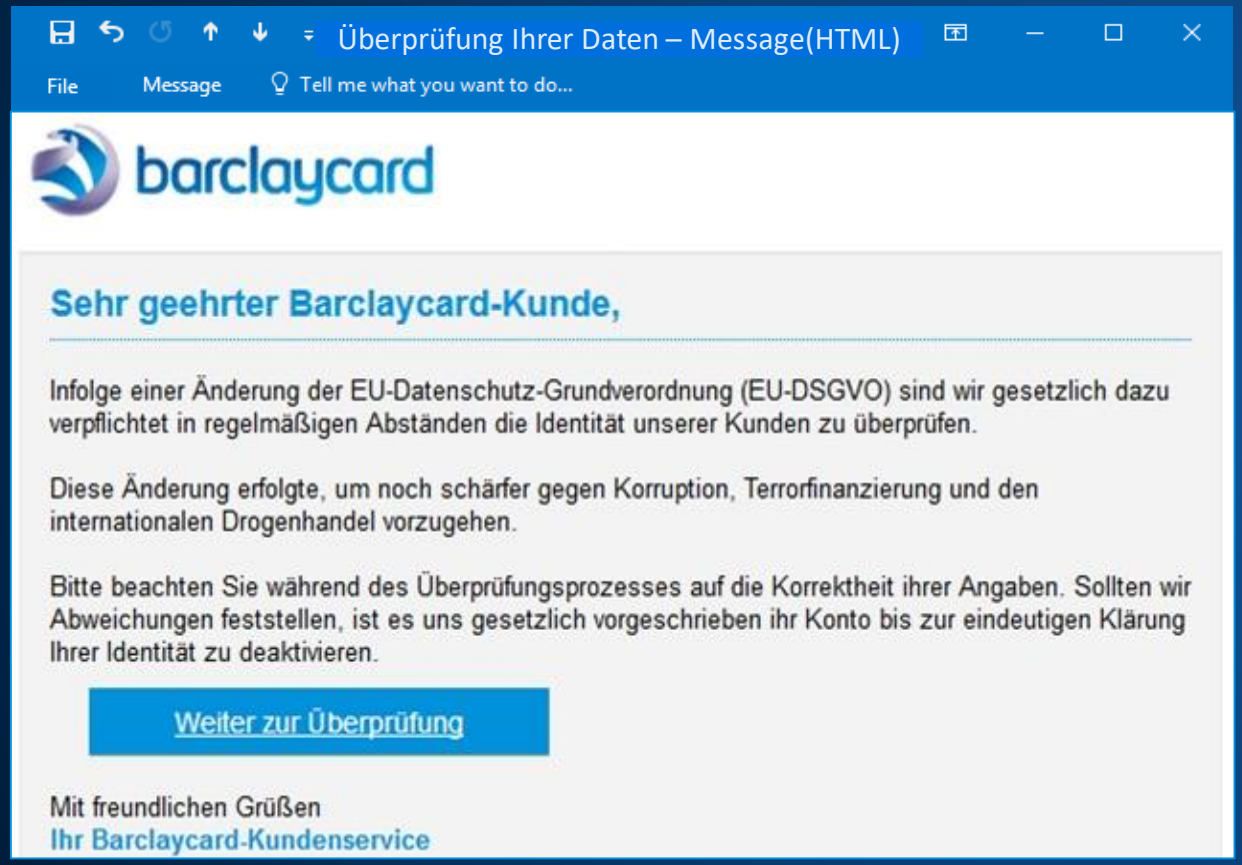
Thanks again. Your licence fee helps keep your old favourites on air, and bring new favourites to life.

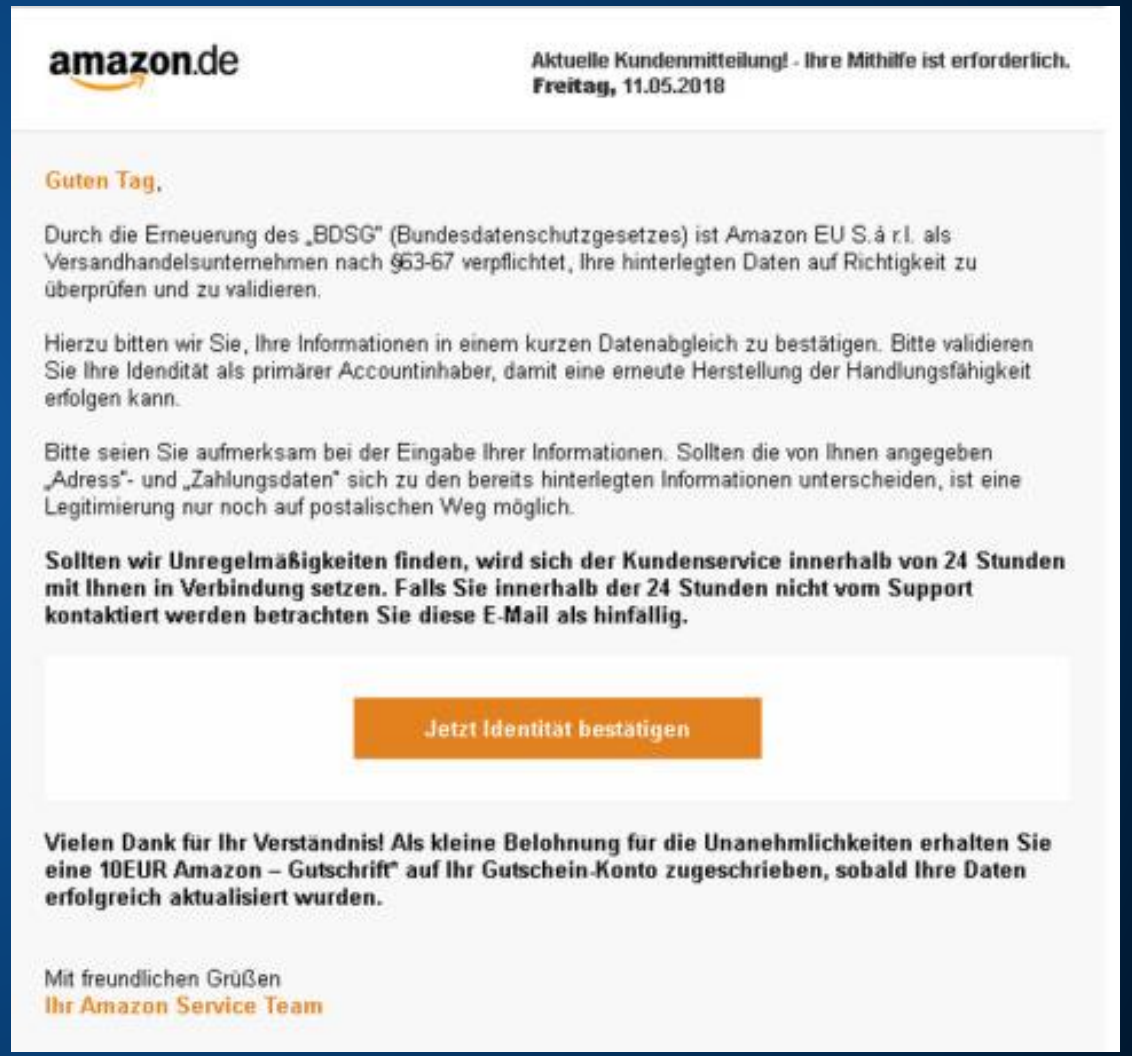
Sign in to your licence

Your TV Licence details:	
Licence number:	
Licence expiry date:	28 February 2018
Surname on licence:	

In the UK
we spend almost 24 hours
a week watching TV

Die EU-DSGVO wird ausgenutzt..





Phishing funktioniert

golem.de IT-NEWS FÜR PROFIS

HOME TICKER VIDEO AUDIO FORUM Suchen

TOP-THEMEN: GDC 2018 Auto Bundeshack Raumfahrt Security Spectre mehr...

SERVICES: PREISVERGLEICH STELLENMARKT TOP-ANGEBOTE IT-KÖPFE GEHALTSCHECK NEWSLETTER ABO

CEO-FRAUD

Autozulieferer Leoni um 40 Millionen Euro betrogen

Mit dem sogenannten Chef-Trick erbeuten Kriminelle oft Millionenbeträge vo
Unternehmen. Mit fingierten E-Mails und Zahlungsanweisungen werden illeg
Geldtransfers eingeleitet. Jetzt hat es einen großen deutschen
Automobilzulieferer getroffen.

Quelle: hg, 17. August 2016, 11:19

Football team pays $2.5 million to criminals in transfer fee scam

29 MAR 2018 2

Spam

Arten von Phishing

Massen
Phishing

Spear
Phishing

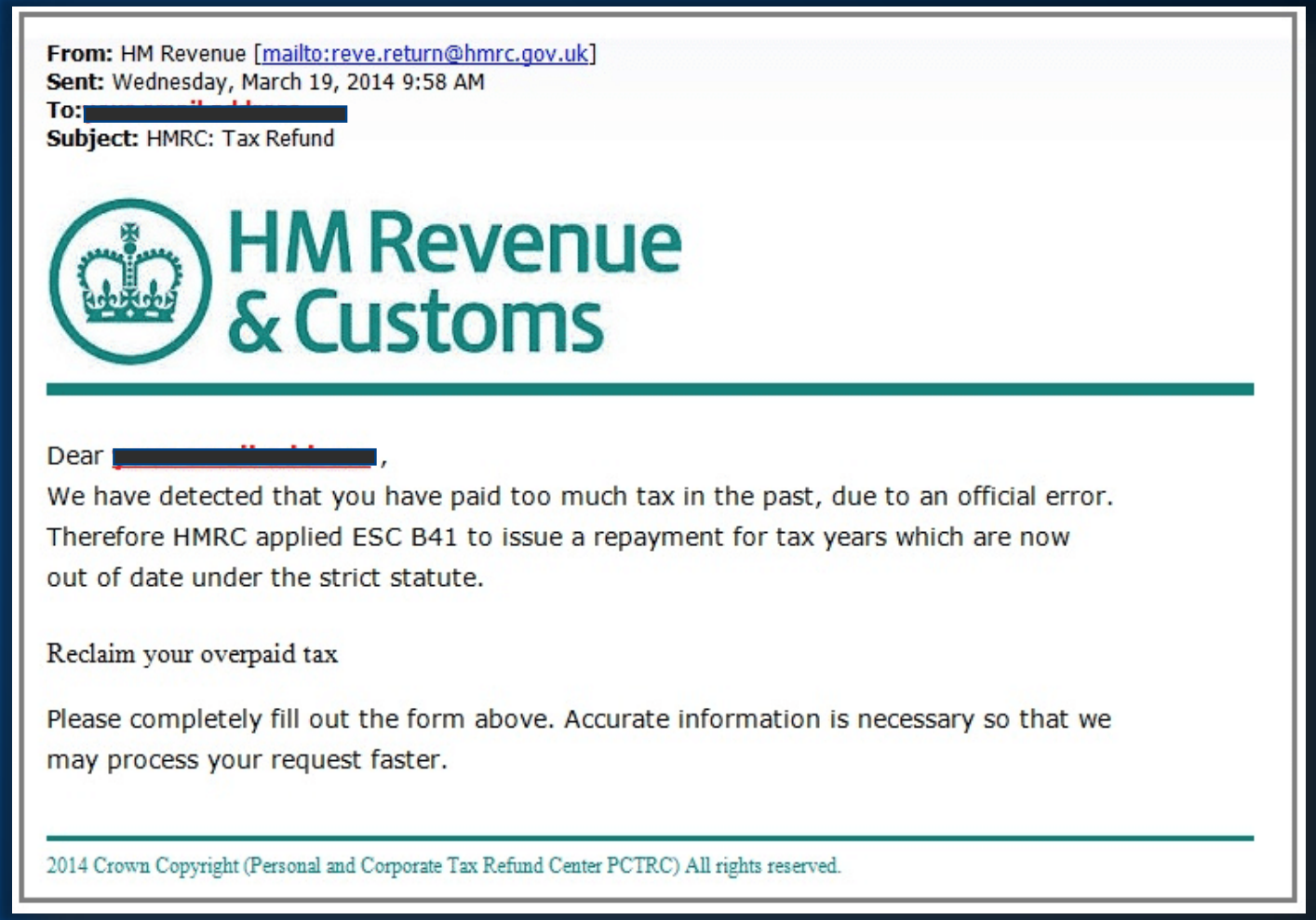
BEC
Phishing

Massen Phishing

- Nutzt bekannte Consumer-Dienste
- Nicht personalisiert
- Dringlichkeit wird suggeriert
- Ziele:
  - Logindaten
  - Kreditkarten-/Bankdaten
- Gestohlene Daten werden direkt genutzt oder verkauft

Spear Phishing

- Zielen auf einzelnen Mitarbeiter oder Mitglieder einer Gruppe eines Unternehmens
- Verwenden gespoofte / echt aussehende Absendeadressen
- Angreifer tritt als vertrauens-würdige Instanz oder hochrangiger Vorgesetzter auf
- Varianten: CEO Fraud, Business Email Compromise (BEC)



From: HM Revenue [mailto:reve.return@hmrc.gov.uk]
Sent: Wednesday, March 19, 2014 9:58 AM
To: [redacted]
Subject: HMRC: Tax Refund

HM Revenue & Customs

Dear [redacted],

We have detected that you have paid too much tax in the past, due to an official error. Therefore HMRC applied ESC B41 to issue a repayment for tax years which are now out of date under the strict statute.

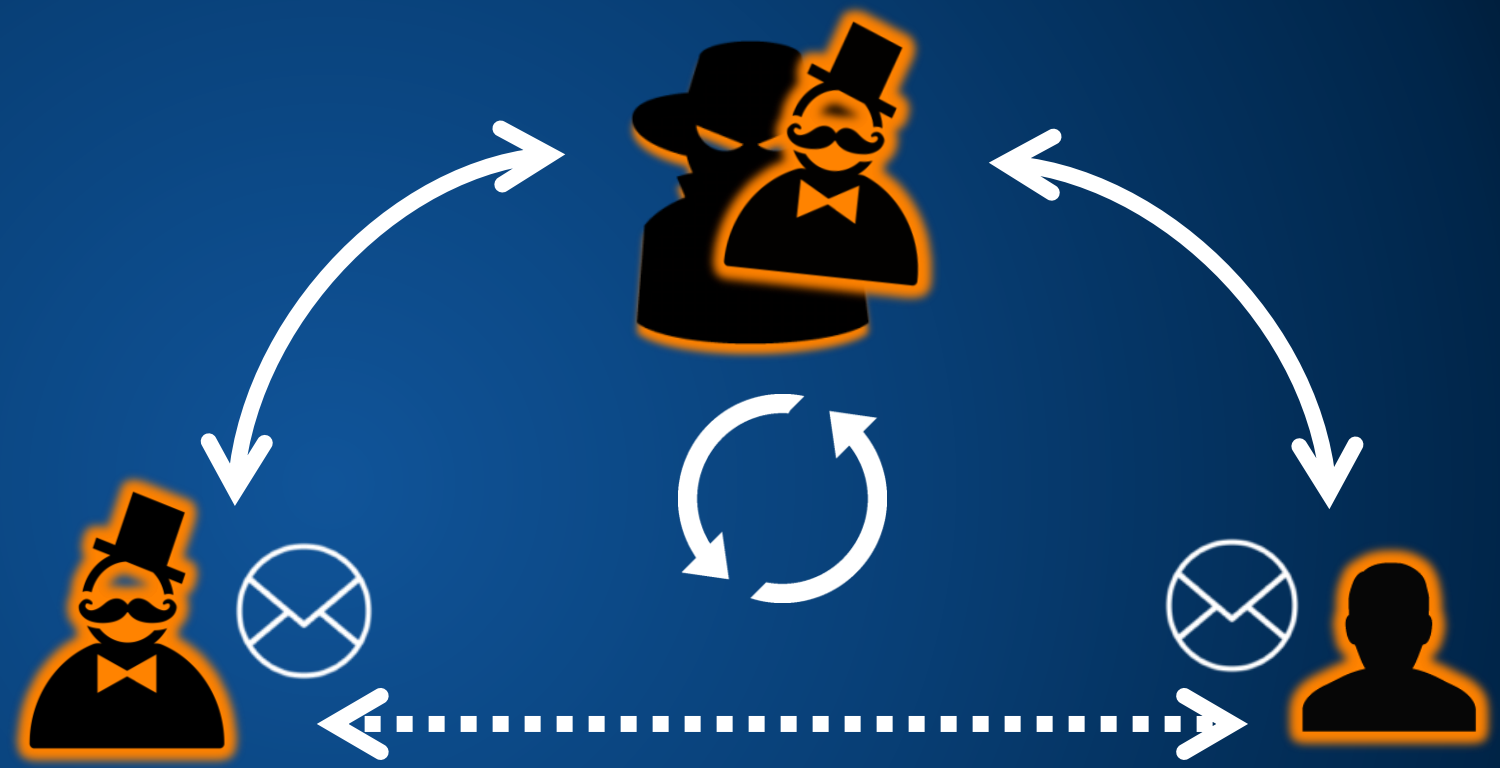
Reclaim your overpaid tax

Please completely fill out the form above. Accurate information is necessary so that we may process your request faster.

BEC Phishing

- Übernahme des Profils inkl. Emailkonto von hochrangiger Person, oft durch Exploits
- Kommunikation sieht für das Opfer täuschend echt aus
- Angreifer überwacht und verändert Kommunikation z.B. Kontodaten für echtes Geschäft
- oder Angreifer täuscht Vorgang komplett vor

Absender: Look-a-like Email-Adresse
oder kompromittierte CEO Mailbox



CEO
CEO schickt angeblich Email

Opfer
Opfer sieht Email des CEO, schickt Antwort an Angreifer

Schutz gegen moderne Email-Bedrohungen

Schutz am Gateway

Email & Web Schutz

- Anti-Virus & Anti-SPAM
- Machine Learning
- URL-Filterung
- Time-of-click URL Schutz
- Sandboxing

Schutz am Endpoint

Endpoint-Schutz

- Anti-Malware
- Machine Learning
- Anti-Exploit
- Anti-Ransomware
- Anti-Hacker

Schutz gegen moderne Email-Bedrohungen

Schutz am Gateway

Email & Web Schutz

- Anti-Virus & Anti-SPAM
- Machine Learning
- URL-Filterung
- Time-of-click URL Schutz
- Sandboxing

Benutzer-Training

Angriffs-Simulation

- Training
- Überprüfung
- Reporting

Schutz am Endpoint

Endpoint-Schutz

- Anti-Malware
- Machine Learning
- Anti-Exploit
- Anti-Ransomware
- Anti-Hacker

Was ist Sophos Phish Threat?

Benutzer-Training

Überprüfung

Reporting

SOPHOS

EVOLVE

Demo

PhishThreat

SOPHOS
CENTRAL
Admin

Übersicht

- Dashboard
- Alarme
- Bedrohungsanalyse-Center
- Protokolle & Berichte
- Personen
- Geräte
- Globale Einstellungen
- Geräte schützen

MEINE PRODUKTE

- Endpoint Protection
- Server Protection
- Mobile
- Encryption
- Web Gateway
- Wireless
- Email Gateway
- Firewall-Verwaltung

Sophos Central Dashboard

Snapshot Ihrer Schutzmaßnahmen anzeigen

Hilfe · Michael Veit
Sophos Ltd · Superadmin

Letzte Alarme

Alle Alarme anzeigen

Es liegen derzeit keine Alarme vor.

Geräte und Benutzer: Übersicht

Bericht anzeigen

Aktivitätsstatus Endpoint-Computer

- **11** Aktiv
- **2** Inaktiv 2+ Wochen
- **21** Inaktiv 2+ Monate
- **1** Nicht geschützt

Web Control für Endpoint und Server

Berichte anzeigen

4 Web-Bedrohungen Blockiert	**2** Richtlinienverstöße Blockiert
0 Richtlinien-Warnungen Ausgegeben	**0** Richtlinien-Warnungen Fortgefahren

Letzte 30 Tage

Übersicht über Web Gateway-Blockierungen

Bericht anzeigen

7 T | 14 T | 30 T

0
Insgesamt blockiert

Keine Blockiermaßnahmen gemeldet. Aktualisieren Sie Ihre Web Gateway-Richtlinie, um die blockierten Daten anzuzeigen.

Email Security

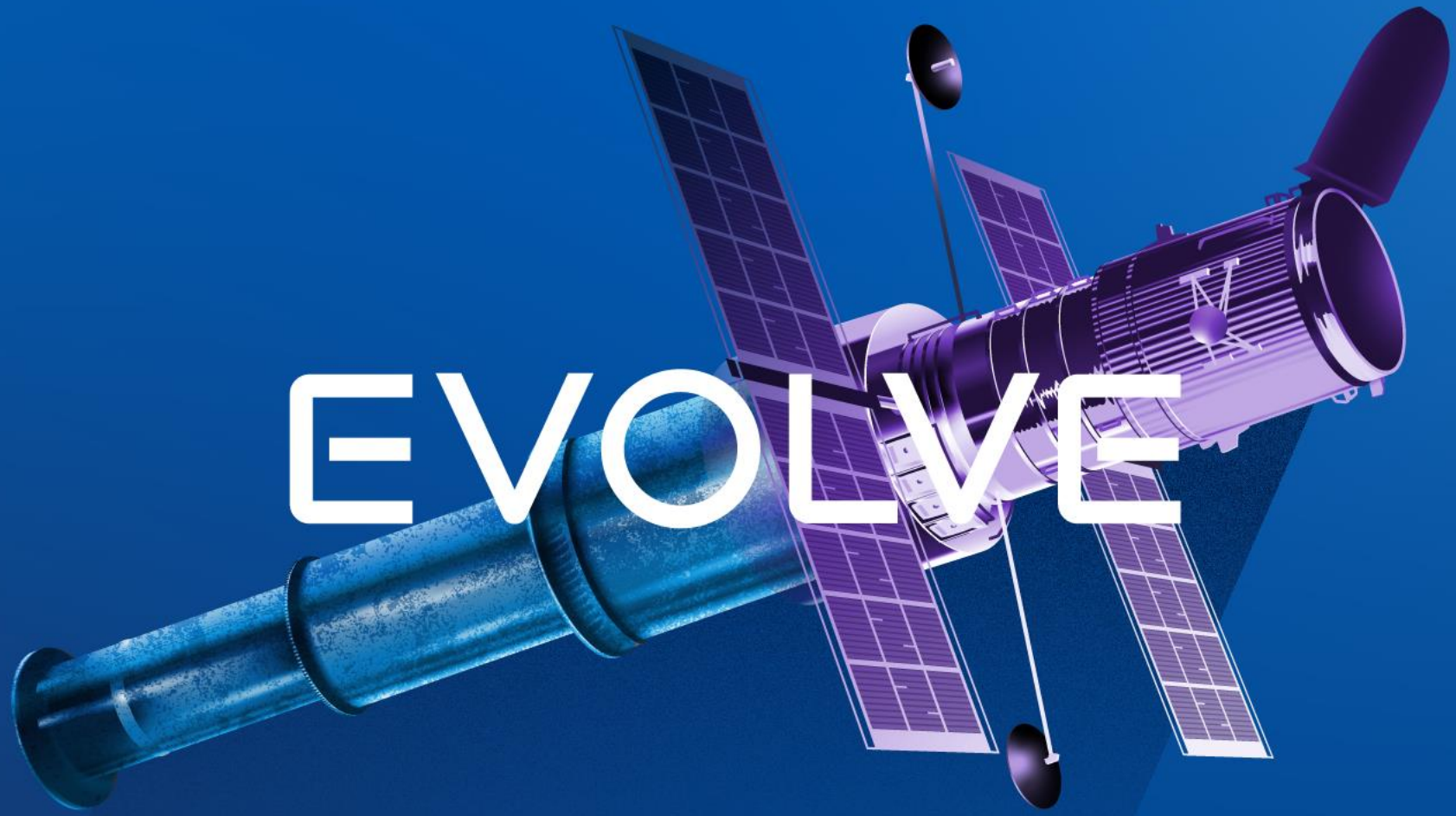
Bericht anzeigen

Eingehend | Ausgehend

4 Gescannte E-Mails
16 Gescannte Posteingänge

- **0** Spam
- **0** DLP-Richtlinienverstöße
- **0** Viren
- **0** Authentifizierungsfehler
- **0** Echtzeit-Blocklist
- **0** Unternehmens-Blocklist

Fragen?



EVOLVE

SOPHOS

ROADSHOW 2019