

# IT-Sicherheit

---

## STAND DER TECHNIK 2021

19. Oktober 2021

Marco Rossi



# Inhalt



- ⊕ **About**
- ⦿ **Worüber man spricht**
- ☀ **Was man meint**
- 📍 **Was man hat**
- 🔄 **Was möglich ist**
- 🔄 **Was man tun kann**
- ⦿ **Was man wissen sollte**
- ⚡ **Top Themen 2021/2022**
- Z **Rapid Risk Assessment**



● Global Security Operation Center  
● SpiderLabs Research Center



250+

Threat hunters, ethical hackers, investigators and researchers in Trustwave SpiderLabs



2,000+

Security-minded employees worldwide



96 Countries

Global Trustwave customer footprint



9

Security Operations Centers



# Worüber man spricht



Hast Du das mit der Firma ... gelesen?

Gab es bei euch auch schon einen Vorfall?

War es eine Erpressung?

Habt Ihr bezahlt?

Was wurde gestohlen?

Wo waren die Lücken?

## Flugzeugbau-Zulieferer stoppt Produktion – Verdacht auf Ransomware

Die belgische Firma ASCO Industries leidet seit Freitag unter einer nicht näher spezifizierten Attacke, die ihre Produktion zum Erliegen gebracht hat.

The screenshot shows the ASCO Industries website. At the top, there is a banner with the text "PRECISION PRODUCTS" over a background image of an airplane. Below the banner, there are three main navigation sections: "ABOUT ASCO", "CAREERS", and "LOCATIONS".

**ABOUT ASCO**

ASCO is a world class supplier of design and manufacture of high lift structures, complex mechanical assemblies and major functional components. We are passionate about precision in our products and in our [relationships](#). Our rich history and understanding of market needs merges with our knowledge of technology in the aerospace industry. Our passion provides clarity and focus in supporting our customers with collaborative development [projects](#).

› [Learn more about ASCO](#)  
› [ASCO Corporate Presentation](#)

**CAREERS**

It is our ambition to continuously expand our capabilities and to grow our business through innovative and competitive offerings to the customer. If you want to be part of the ASCO venture and to commit to the [ASCO values](#), we would be happy to receive your [application](#).

› [Show all open vacancies](#)

**LOCATIONS**

[Leonardo said...](#)  
Humanism and inventiveness  
Underscored by a true passion  
For technique and precision...

[ASCO Industries nv/sa](#)  
Weveldaan 2  
1930 Zaventem, Belgium  
+32 2 716 06 11  
[View contact page](#)

Copyright © 2019 ASCO Industries  
We use cookies to provide analytics.

# Was man meint



**Hoffentlich passiert uns so etwas nicht!**

**Was müsste ich dafür tun?**

**Wie soll ich die Kosten begründen?**

## Norddeutsche Finanzämter: IT-Ausfall und Trojaner-Prävention

Seit Dienstagnacht sind Finanzämter im Norden von einem IT-Ausfall betroffen. Zudem lehnt Niedersachsens Finanzverwaltung E-Mails mit Office-Anhang ab.

## NotPetya: Zurich will Schäden nicht bezahlen, weil Angriff "kriegsähnlich" war

Zurich will die Schäden nicht bezahlen, die NotPetya bei Mondelēz angerichtet hat. Die Versicherung deckt keine staatlichen Angriffe.

F.A.Z. EXKLUSIV

# Cyberkriminelle erpressen Krauss Maffei

# Was man hat



**Gerade vor einem Jahr haben wir die neuen Firewalls mit noch mehr Leistung für viel Geld gekauft!**

**Sind denn Firewalls, Anti-Virus und Proxy-Server noch immer nicht genug?**

heise online › News › 03/2021 › **Jetzt patchen! Angreifer attackieren Microsoft Exchange Server**

 Alert!

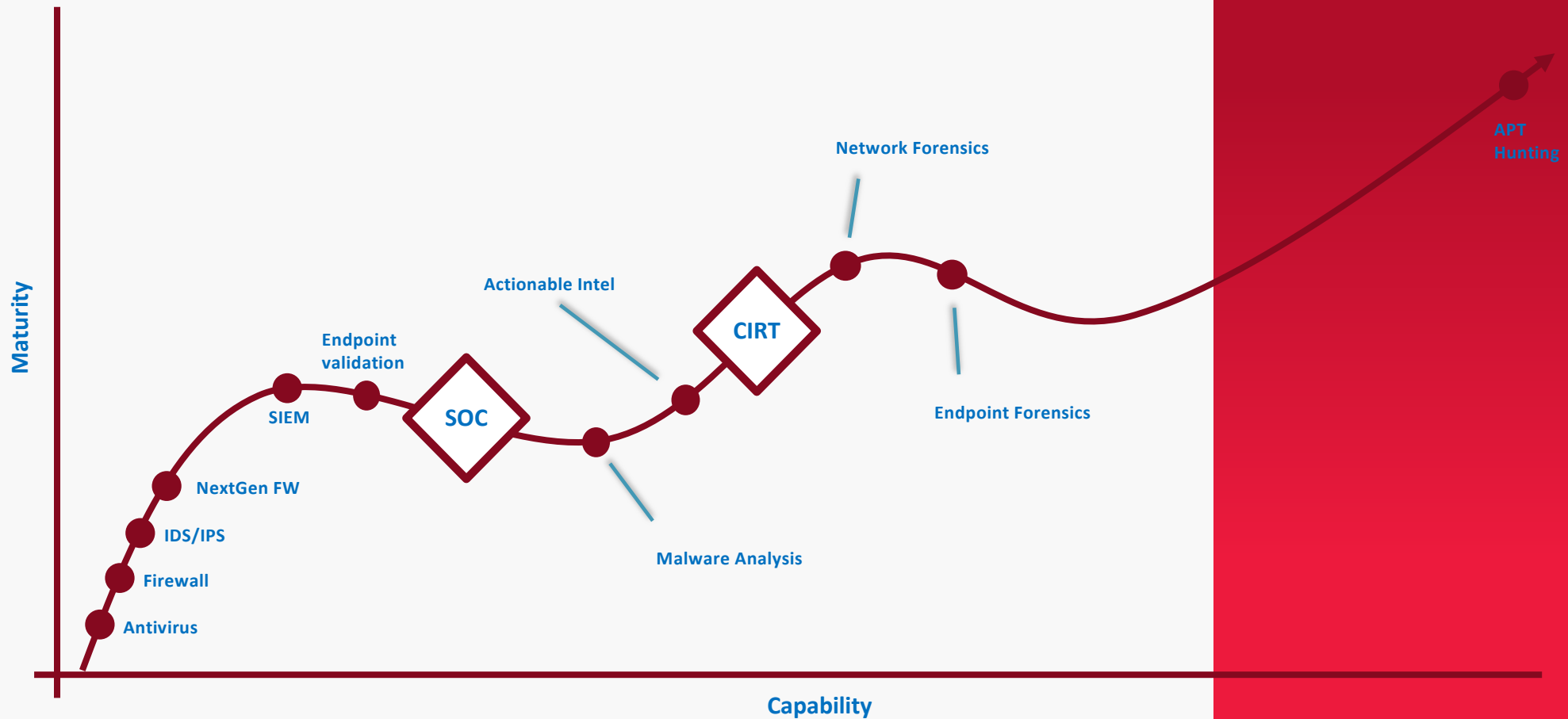
**Jetzt patchen! Angreifer attackieren Microsoft Exchange Server**

## Fake-Bewerbungsmails: Trojaner versteckt sich erfolgreich vor Antiviren-Software

Derzeit rollt eine neue Welle von Fake-Bewerbungen durch das Internet. Ziel ist es, den Erpressungstrojaner Gandcrab auf Computer zu bringen.



# Was möglich ist

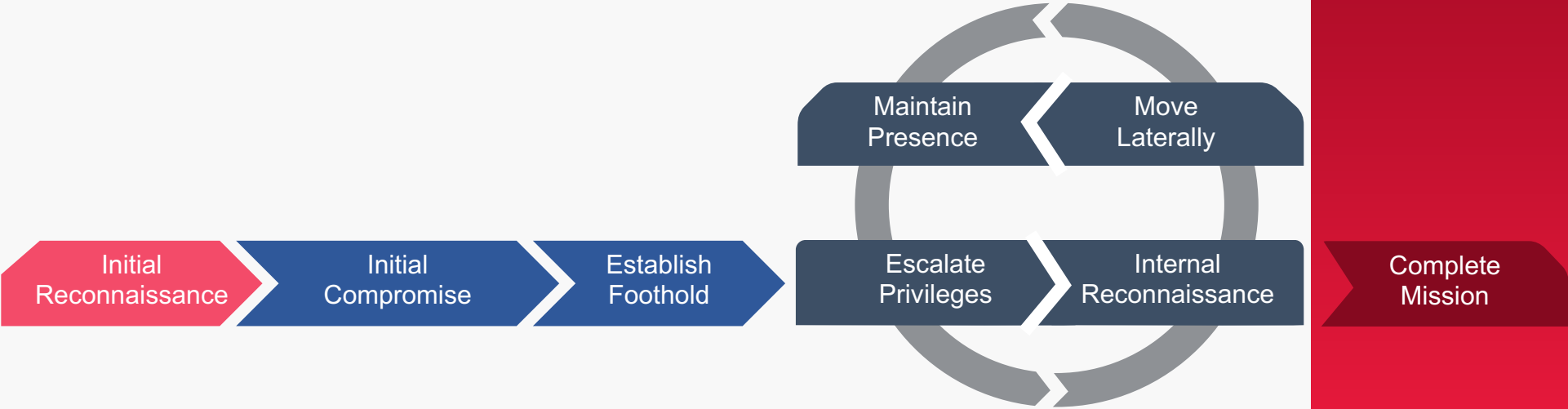


■ Überblick





# Wie Angriffe erfolgen



## ▪ Killchain



# SpiderLabs Telemetry Report 2021

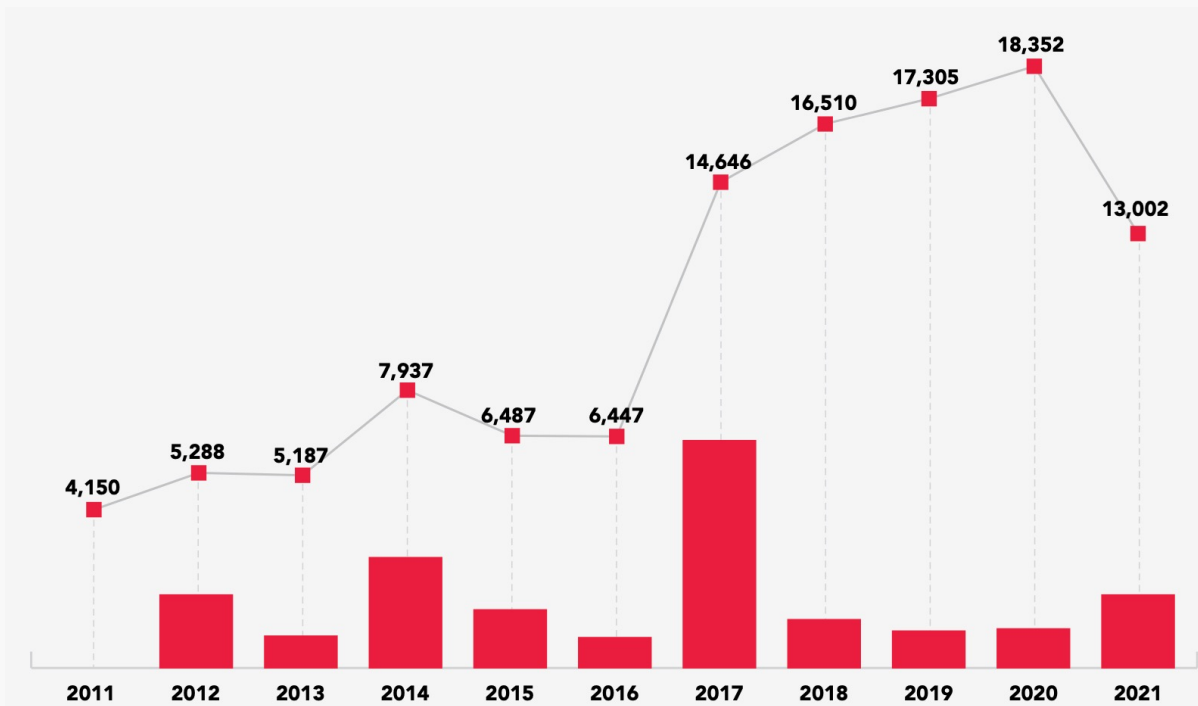


Figure 1: Number of vulnerabilities published in NVD from 2011-2021 (As of September 1, 2021)



## 2021 Trustwave SpiderLabs Telemetry Report

The State of High-Profile Vulnerabilities

# SpiderLabs Telemetry Report 2021

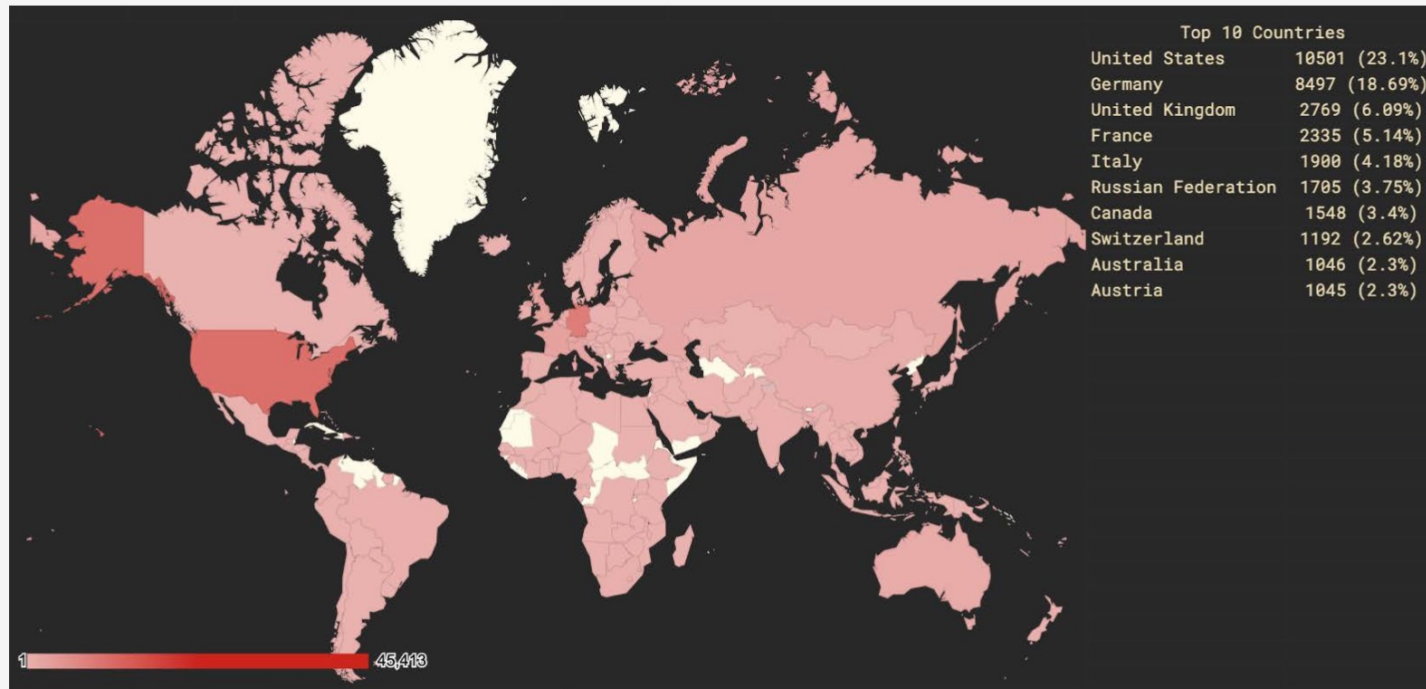


Figure 6: Heatmap of Exchange Servers vulnerable to ProxyShell (As of August 31, 2021)



## 2021 Trustwave SpiderLabs Telemetry Report

The State of High-Profile Vulnerabilities

# SpiderLabs Telemetry Report 2021

## Top 10 Countries

Germany	6512 (23.40%)
United States	5999 (21.56%)
United Kingdom	1709 (6.14%)
France	1437 (5.16%)
Italy	1149 (4.13%)
Canada	958 (3.44%)
Austria	926 (3.33%)
Switzerland	873 (3.14%)
Russian Federatior	730 (2.62%)
Netherlands	683 (2.45%)



## 2021 Trustwave SpiderLabs Telemetry Report

The State of High-Profile Vulnerabilities

# Was man tun kann

## ■ Organisation und Strukturen

- 4 Augenprinzip für neue Firewall-Regeln
- Rechte & Rollenmodell überprüfen
- Mind. eine IT-Sicherheitsfachkraft (nicht nur Verantwortlichen)
- Netzwerksegmentierung (IT/OT)



# Was man tun kann

## ■ Technologie Update

- E-Mail Sicherheitsgateways mit dynamischer (Sandbox, URL-Links in E-Mails ins Echtzeit, Retrospektive Alarmierung) Analyse
- NextGenAV (ML/AI) optional gleich mit EDR-Technologie
- SSL-Interception
- 2 Faktor Authentifizierung
- Zentrale Logdatenerfassung (SIEM, opt. mit SEC-Analyse)





# Was man wissen sollte

- **Jede neue Technologie bedeutet Aufwand**
  - Implementierung & Betrieb
  - Lösungen die „Zero-Administration“ versprechen sollte man sich genau anschauen
  - Je “vielversprechender“ die Lösungen sind, um so höher ist oftmals die False-Positive Rate und damit der personelle Aufwand



# Was man wissen sollte

- **Trotz aller technischen Schutzmaßnahmen ist es nur eine Frage der Zeit bis etwas passiert**
  - Heute schon an morgen denken
  - Notfallplan und Notfallübungen
  - Kontaktadresse zu externen IT-Sicherheitsspezialisten, die bei einem Vorfall helfen können



# Alternativ bzw. Additiv

- **Auslagern von...**
  - personalintensiven Cyber Security Aufgaben
  - High Level Expertise
  - 24/7 Überwachung
  - „Co-Managed SOC“
  - Managed Detection and Response (MDR)





# Meine Top Themen 2022

## ■ Ransom(ware)

- „Zufällig“, über eine Schwachstelle im System
- Gezielt, um Daten zu „entführen“ (verschlüsseln)

### Computerattacke auf Norsk Hydro

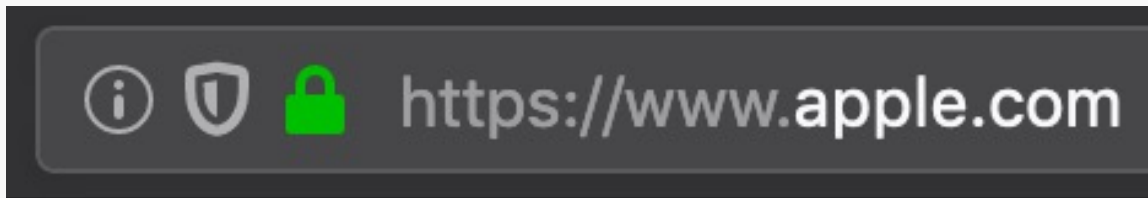
## **Angreifer legten Alu-Konzern mit Erpressersoftware lahm**


Der Aluminiumhersteller Norsk Hydro wurde Opfer eines Cyberangriffs mit Ransomware. Die Angreifer wollten den Konzern offenbar mit einer längst bekannten Schadsoftware erpressen.

# Meine Top Themen 2021/2022

## ■ Phishing

- Klassisches Abgreifen von vertraulichen Informationen
- CEO Fraud aka Business Email Compromise (BEC) aka Impersonation

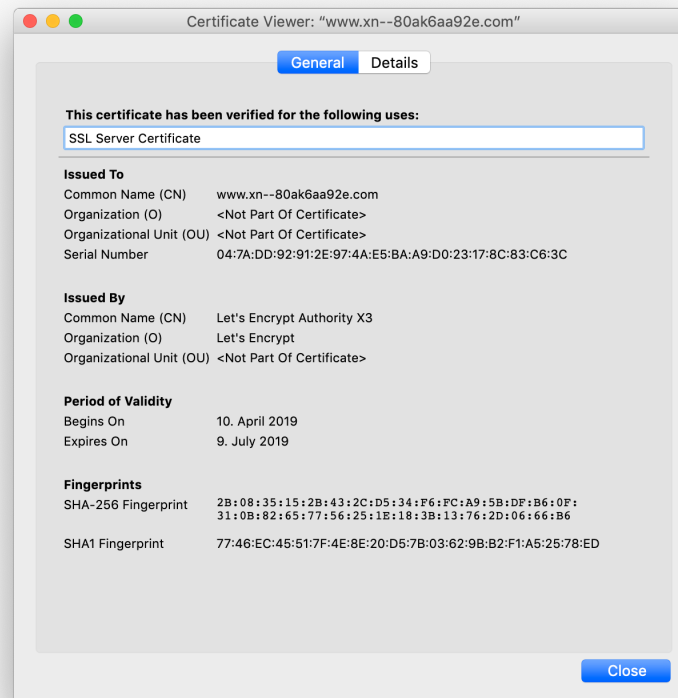



- Gilt zum Glück nicht für alle Browser! 

# Meine Top Themen 2021/2022

## ■ Phishing

- Klassisches Abgreifen von vertraulichen Informationen
- CEO Fraud aka Business Email Compromise (BEC) aka Impersonation

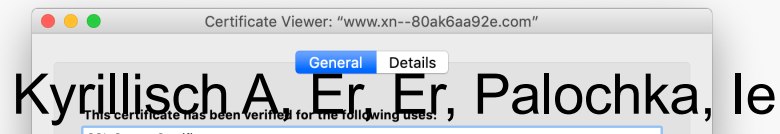


- Gilt zum Glück nicht für alle Browser! 

# Meine Top Themen 2021/2022

## ■ Phishing

- Klassisches Abgreifen von vertraulichen Informationen
- CEO Fraud aka Business Email Compromise (BEC) aka Impersonation



### Issued To

Common Name (CN)	www.xn--80ak6aa92e.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	04:7A:DD:92:91:2E:97:4A:E5:BA:A9:D0:23:17:8C:83:C6:3C

### Fingerprints

SHA-256 Fingerprint	2B:08:35:15:2B:43:2C:D5:34:F6:FC:A9:5B:DF:B6:0F: 31:0B:82:65:77:56:25:1E:18:3B:13:76:2D:06:66:B6
SHA1 Fingerprint	77:46:EC:45:51:7F:4E:8E:20:D5:7B:03:62:9B:B2:F1:A5:25:78:ED

Close

- Gilt zum Glück nicht für alle Browser!



# Meine Top Themen 2021/2022

## ■ Phishing

- Klassisches Abgreifen von vertraulichen Informationen
- CEO Fraud aka Business Email Compromise (BEC) aka Impersonation

Kyrillisch A, Er, Er, Palochka, le

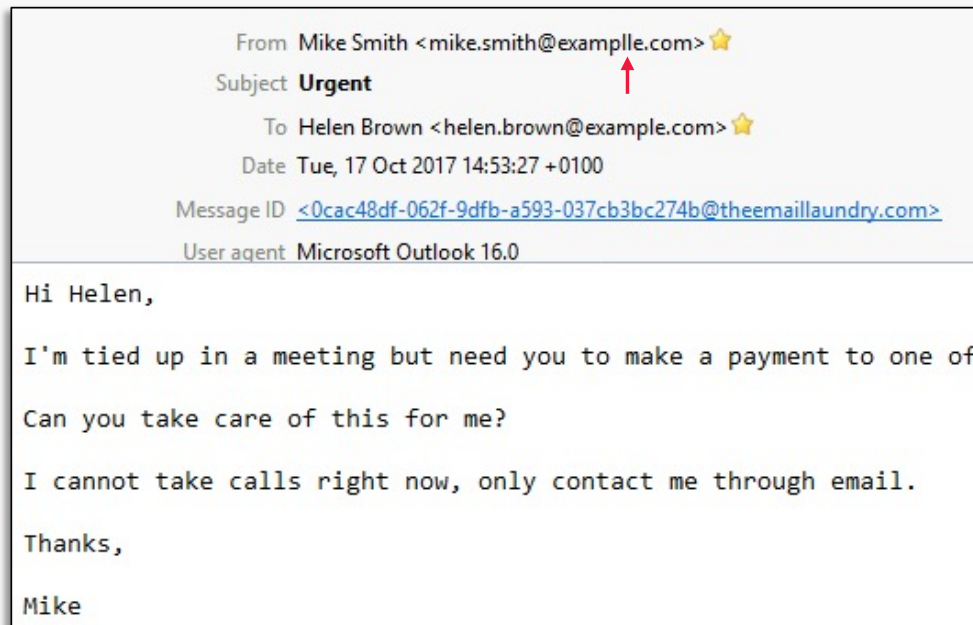
### Issued To

Common Name (CN)	www.xn--80ak6aa92e.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	04:7A:DD:92:91:2E:97:4A:E5:BA:A9:D0:23:17:8C:83:C6:3C

- Gilt zum Glück nicht für alle Browser!



# Was macht “Impersonation” so erfolgreich?



# Was macht "Impersonation" so erfolgreich?

From Mike Smith <[ceofraud71286@gmail.com](mailto:ceofraud71286@gmail.com)> ☆  
Subject **Urgent**  
To Helen Brown <[helen.brown@example.com](mailto:helen.brown@example.com)> ☆  
Date Tue, 17 Oct 2017 15:05:38 +0100  
Message ID <[fb471d53-2440-b5f8-d2fd-bd3a27be5a69@theemailaundry.com](mailto:fb471d53-2440-b5f8-d2fd-bd3a27be5a69@theemailaundry.com)>  
User agent Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Thunderbird

Hi Helen,

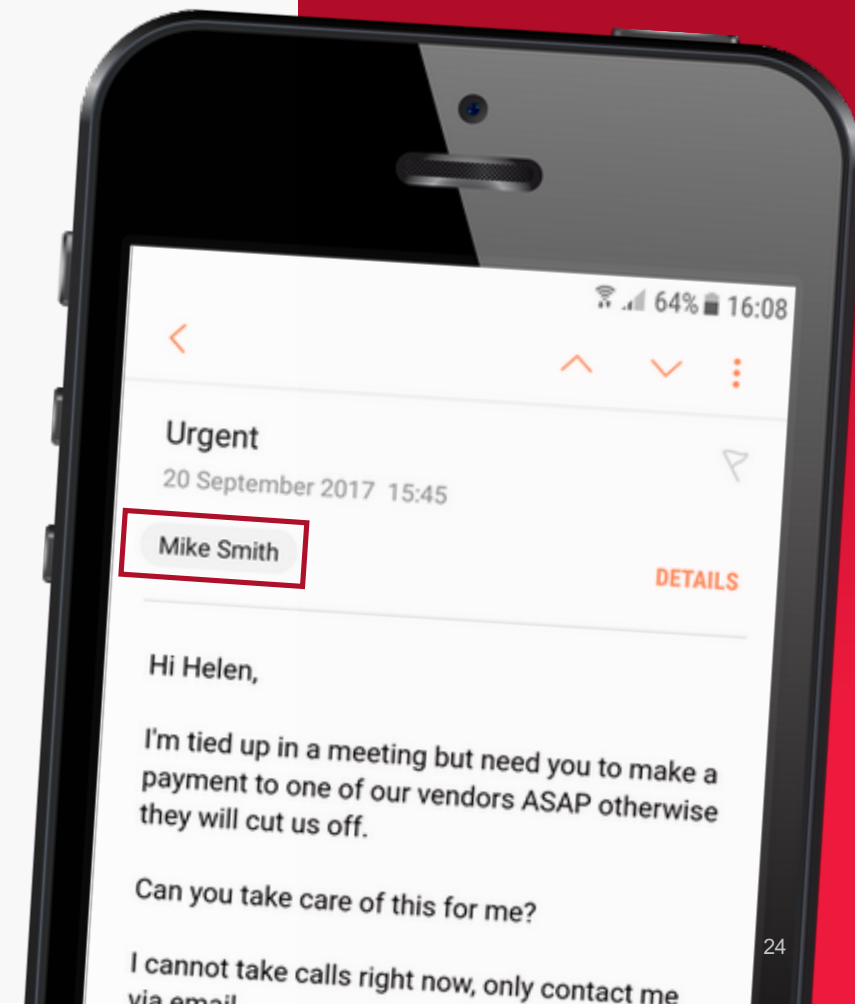
I'm tied up in a meeting but need you to make a payment to one of our vendors ASAP otherwise they will cut us off.

Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike





# Was macht "Impersonation" so erfolgreich?

From mike.smith@example.com <[ceofraud71286@gmail.com](mailto:ceofraud71286@gmail.com)>  
Subject **Urgent**  
To Helen Brown <[helen.brown@example.com](mailto:helen.brown@example.com)> ★  
Date Tue, 17 Oct 2017 15:05:38 +0100  
Message ID <[fb471d53-2440-b5f8-d2fd-bd3a27be5a69@theemaillaundry.com](mailto:fb471d53-2440-b5f8-d2fd-bd3a27be5a69@theemaillaundry.com)>  
User agent Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Thunderbird

Hi Helen,

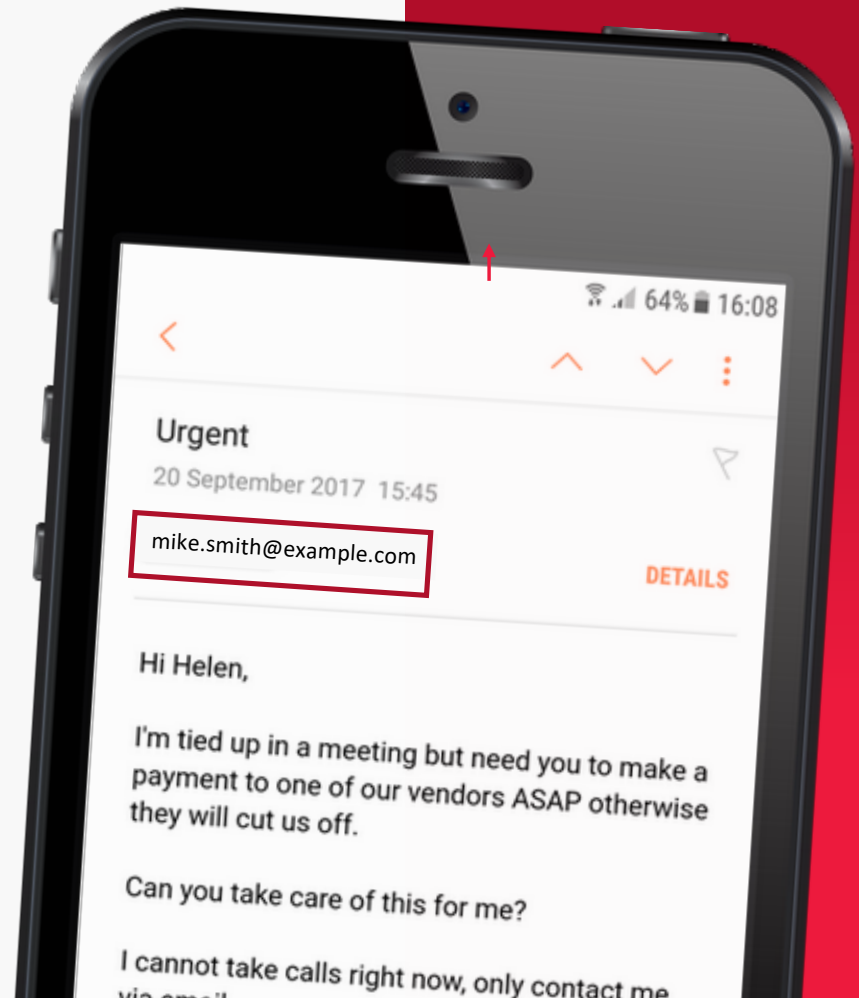
I'm tied up in a meeting but need you to make a payment to one of our vendors ASAP otherwise they will cut us off.

Can you take care of this for me?

I cannot take calls right now, only contact me through email.

Thanks,

Mike



# Rapid Risk Assessment

```
Eingabeaufforderung
C:\Users>ping spiegel.de
Ping-Anforderung konnte Host "spiegel.de" nicht finden. Überprüfen Sie den Namen
, und versuchen Sie es erneut.
C:\Users>_
```

## ■ Selbsttest



– Hervorragend

# Rapid Risk Assessment

```
Eingabeaufforderung
C:\Users>ping spiegel.de

Ping wird ausgeführt für spiegel.de [128.65.210.8] mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 128.65.210.8:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100% Verlust),

C:\Users>_
```

## ■ Selbsttest

– Schwach



# Rapid Risk Assessment

```
Eingabeaufforderung
C:\Users>ping spiegel.de

Ping wird ausgeführt für spiegel.de [128.65.210.8] mit 32 Bytes Daten:
Antwort von 128.65.210.8: Bytes=32 Zeit=10ms TTL=128
Antwort von 128.65.210.8: Bytes=32 Zeit=9ms TTL=128
Antwort von 128.65.210.8: Bytes=32 Zeit=10ms TTL=128
Antwort von 128.65.210.8: Bytes=32 Zeit=12ms TTL=128

Ping-Statistik für 128.65.210.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 9ms, Maximum = 12ms, Mittelwert = 10ms

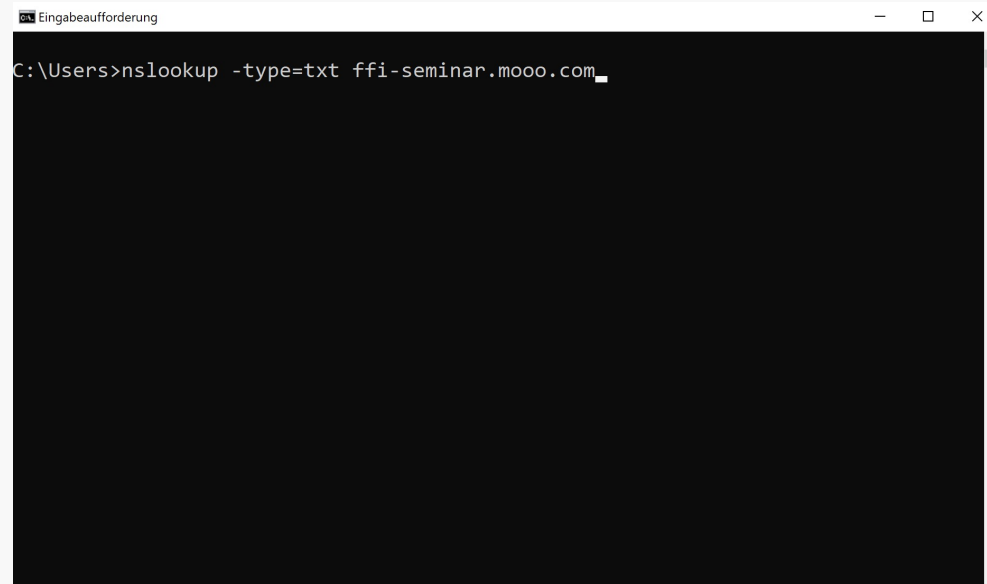
C:\Users>
```

## ■ Selbsttest



– Schlecht

# Rapid Risk Assessment



```
Eingabeaufforderung
C:\Users>nslookup -type=txt ffi-seminar.mooc.com
```

## ■ Selbsttest



– Bonus

# Weiterführende Informationen

- <https://www.trustwave.com/en-us/resources/library/documents/2021-trustwave-spiderlabs-telemetry-report/>
- <https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/>
- <https://www.trustwave.com/en-us/resources/library/documents/2021-network-security-report/>
- <https://www.trustwave.com/en-us/resources/library/documents/2021-email-threat-report/>
- <https://www.securitycolony.com>





# Vielen Dank...



**Marco Rossi**

Senior Sales Engineer

Trustwave Germany GmbH  
The Squire 12  
60549 Frankfurt/Main  
Germany

Mobile +49 172 2942677

marco.rossi@trustwave.com

[trustwave.com](http://trustwave.com)