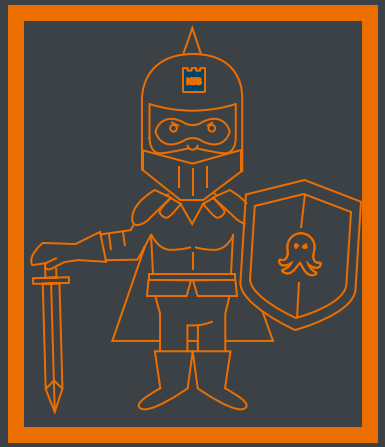

NTS
RELAX,
WE CARE

SUPER MARIO‘S ODYSSEY

Dominik Mocher | Security Architect

VORSTELLUNGSRUNDE

VORSTELLUNGSRUNDE



Name: Daniel Defense

Nickname: d3fc0n0

Alter: 24

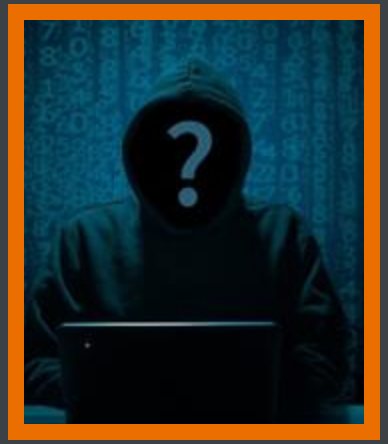
Gewicht: 76 kg

Größe: 176cm

Besondere Fähigkeiten: Memory Forensics, Investigations und CTF Events

Slogan: „*I am always preparing for what's next, not what was last*“

VORSTELLUNGSRUNDE



Name: Anonymous

Nickname: HackMan

Alter: ??

Gewicht: ?? kg

Größe: ??? cm

Besondere Fähigkeiten: Brute Force Angriffe, Command Injection & Social Engineering

Slogan: „*Amateurs hack systems, Professionals hack people*“

ATTACKERS DILEMMA

„Defenders have to get it right **every** time.
Attackers only need to be right **once**.“

„Attackers have to get it right through the **entire attack**. Defenders only need to detect **once**.“

ROUND 1

- FIGHT! -

Shroom Factory AG

Nutrition and Supplements

Raaba-Grambach, Steiermark

3.731 Followerinnen

31 Kontakte sind hier beschäftigt

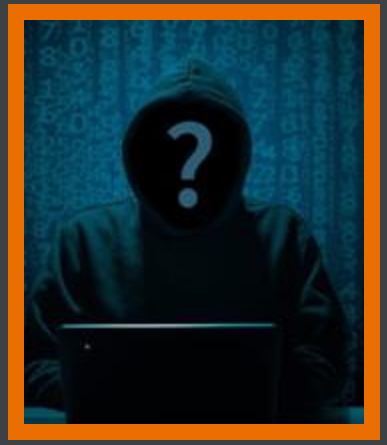
Follower:in | Seite anzeigen

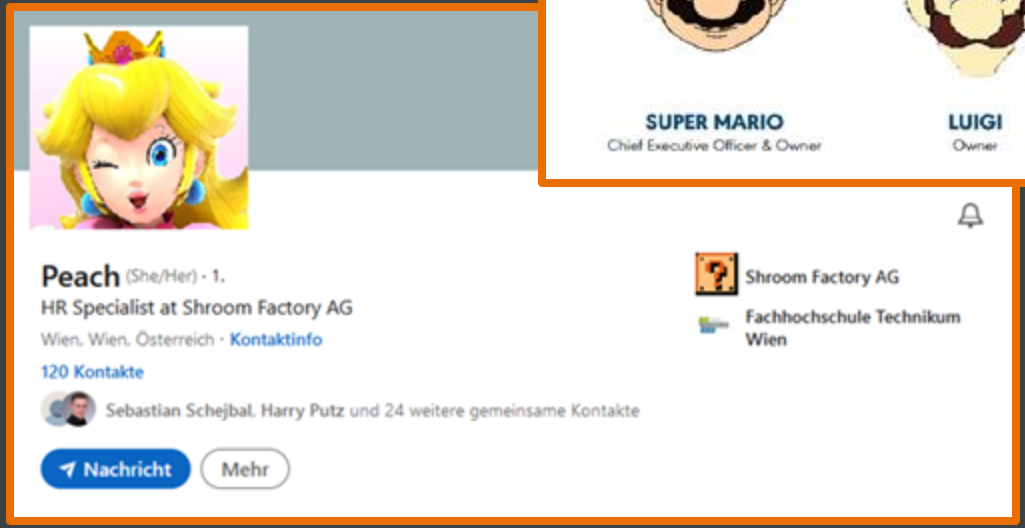
Jobs

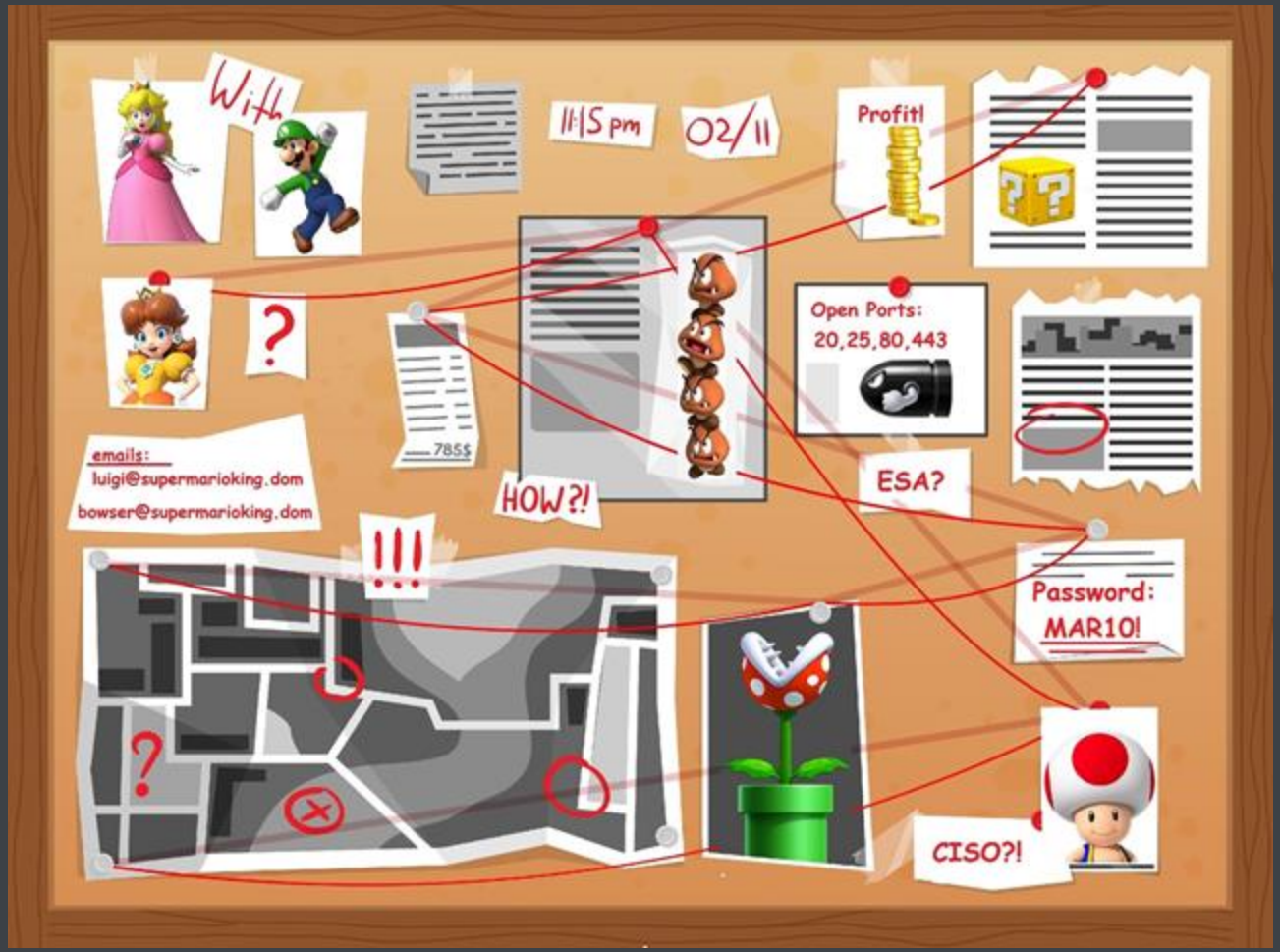
Remote | Einfach bewerben | <10 Bewerbungen

Red Shroom Specialist (m/w/d)
Shroom Factory AG
Innsbruck, Tyrol, Austria (Hybrid)
Vor 1 Woche • 11 Bewerbungen
Speichern

Fire Flower Specialist (m/w/d)
Shroom Factory AG
Graz und Umgebung (Hybrid)
31 Kontakte sind hier beschäftigt
Vor 2 Wochen • 5 Bewerbungen • Einfach bewerben
Speichern






With
11:15 pm
02/11
Profit!
?
Open Ports:
20,25,80,443
emails:
luigi@supermarioking.dom
bowser@supermarioking.dom
785$
HOW?!
ESA?
!!!
Password:
MAR10!
?
CISO?!

Bitte um DRINGENDE Rückmeldung bez. Cloud Migration

Super Mario
An 'yoshi@supermarioking.dom'

office365_activation_link.one
.one-Datei

Hallo Yoshi

It's a me Mario! Ich konnte dich leider telefonisch nicht erreichen!

Anbei übermittle ich dir das Dokument für den Umstieg für die Migration in die Cloud.

Bei Fragen melde dich bitte einfach bei mir!

LG,
Mario

SUPER MARIO
Head of IT

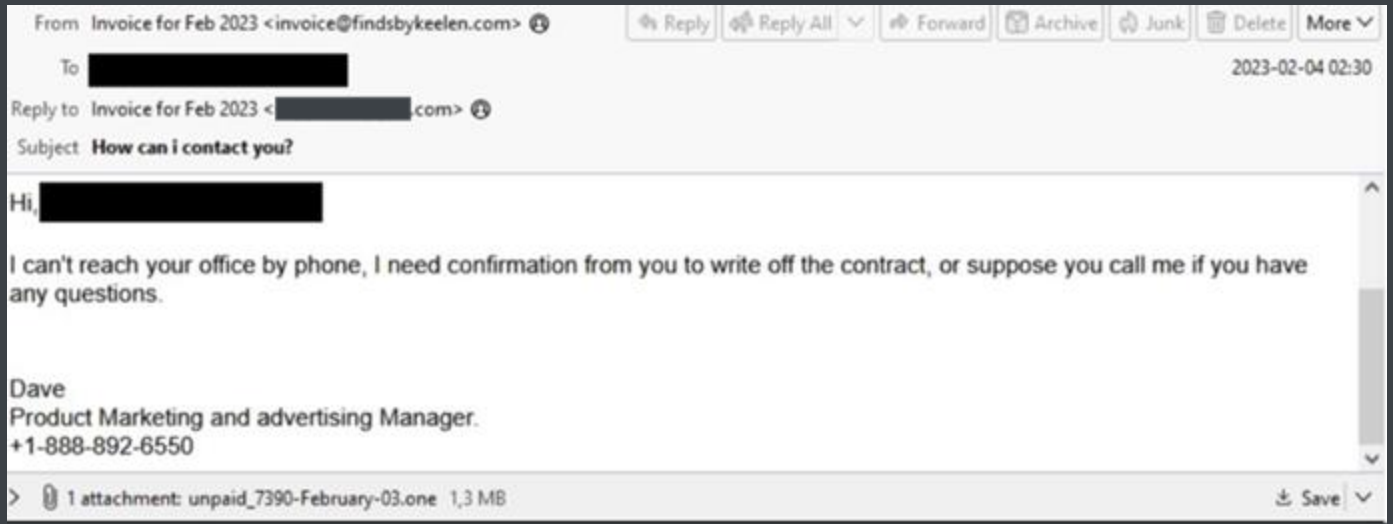
SUPER MARIO BROS. AG
Kingdom Street 1, 1020 Wien

SCHUTZMASSNAHMEN BEI PHISHING

- Immer den Absender / die Absenderadresse überprüfen
- Vorsicht bei Links und Anhängen in Nachrichten!
- Keine Passwörter, Transaktionsnummer, etc. per Mail übermitteln
- Mail-Signaturen und Verschlüsselung verwenden
- Nie auf Phishing-E-Mails antworten

ICEDID – MAIL KAMPAGNE

Originalmail:



RECAP RUNDE 1

- Angreifer sammelte Informationen über sein „Opfer“ erstellt eine Liste von Usern und E-Mail-Adressen
- Einfache Recherche über Suchmaschinen meist ausreichend
- Metadaten von Dateien enthalten oft sensible Informationen
- Malicious Mail wurde an eine Vielzahl von zuvor gesammelten E-Mail-Adressen von Mitarbeitern verschickt

ROUND 2

- FIGHT! -

Timestamp	Customer	Event Name	Urgency	Status
2023-05-25 17:28:36 UTC	s3cp4ck	NTSUC-0089-001 - Connection to malicious known IP/domain	medium	New
2023-05-25 17:12:46 UTC	s3cp4ck	NTSUC-0046-001 - Risk object exceeds risk score threshold	low	New
2023-05-25 16:42:22 UTC	s3cp4ck	NTSUC-0038-001 - PowerShell Long Command Line	low	New
2023-05-25 16:38:55 UTC	s3cp4ck	NTSUC-0039-001 - Encoded powershell command executed	low	New
2023-05-25 16:22:03 UTC	s3cp4ck	NTSUC-0074-001 - Rundll32 using non standard export	high	New
2023-05-25 16:22:01 UTC	s3cp4ck	NTSUC-0038-001 - PowerShell Long Command Line	low	New
2023-05-25 16:21:29 UTC	s3cp4ck	NTSUC-0028-001 - Suspicious Mail Attachment	medium	New

DIE NTS DEFENSE QUIZ-SHOW

DIE

NTS DEFENSE

QUIZ-SHOW

50/50

€ 500

Was sollte unser Analyst als nächstes tun?

A: Rechner neu aufsetzen

B: In Panik verfallen

C: Investigation starten

D: LAN Kabel ziehen

DIE

NTS DEFENSE

QUIZ-SHOW

50/50

€ 500

Was sollte unser Analyst als nächstes tun?

A: Rechner neu aufsetzen

B: In Panik verfallen

C: Investigation starten

D: LAN Kabel ziehen

DIE

NTS DEFENSE

QUIZ-SHOW

50/50

€ 1.000

Mit welcher der folgenden Logquellen sollte der Analyst seine Investigation beginnen?

A: Firewall Logs

B: Endpoint Logs

C: E-Mail Logs

D: Proxy Logs

DIE

NTS DEFENSE

QUIZ-SHOW

50/50

€ 1.000

Mit welcher der folgenden Logquellen sollte der Analyst seine Investigation beginnen?

A: Firewall Logs

B: Endpoint Logs

C: E-Mail Logs

D: Proxy Logs

DIE

NTS DEFENSE

QUIZ-SHOW

50/50

€ 2.000

Was sollte Teil des Response Plans sein?

A: Stakeholder informieren

B: Das Einfallstor des Angriffs ausfindig machen

C: Den aktiven Angreifer isolieren

D: Die Zugangsdaten betroffener User resetten

DIE

NTS DEFENSE

QUIZ-SHOW

50/50

€ 2.000

Was sollte Teil des Response Plans sein?

A: Stakeholder informieren

B: Das Einfallstor des Angriffs ausfindig machen

C: Den aktiven Angreifer isolieren

D: Die Zugangsdaten betroffener User resetten

RECAP ROUND 2

- Der Phishing-Mail Ansatz hat super funktioniert und unser Angreifer konnte sich im Netzwerk der Shroom Factory AG festsetzen

- Dem Angreifer war es möglich den Useraccount des Mitarbeiters zu übernehmen, der die Mail öffnete - Yoshi

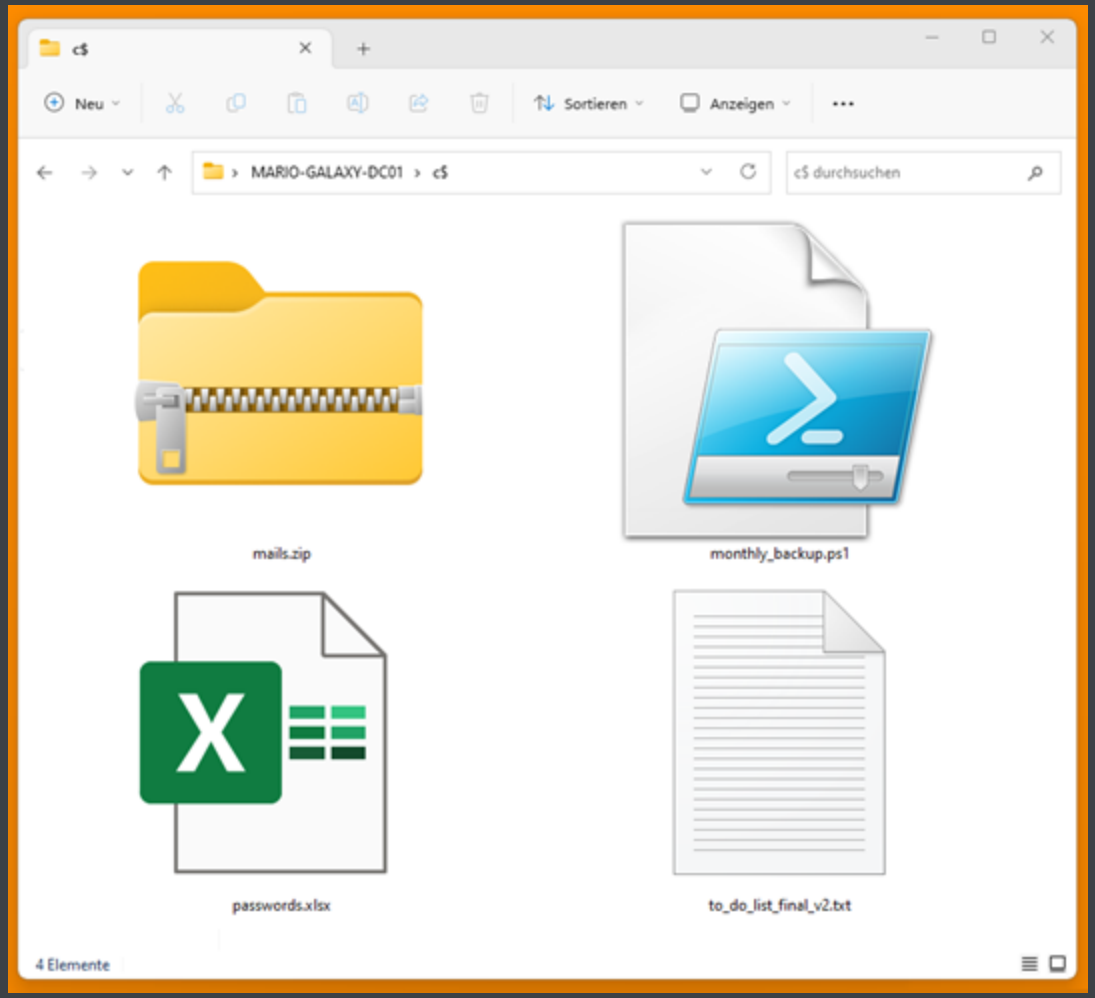
- Des Weiteren versuchte der Angreifer schon einige weitere Useraccounts zu kompromittieren

NTS

ROUND 3

- FINAL ROUND! -

```
str
```


c$
Neu
Sortieren
Anzeigen
MARIO-GALAXY-DC01 › c$
c$ durchsuchen
mails.zip
monthly_backup.ps1
passwords.xlsx
to_do_list_final_v2.txt
4 Elemente

DIE

NTS DEFENSE

QUIZ-SHOW

50/50

€ 4.000

Welche Datei soll unser Angreifer nun genauer betrachten?

A: passwords.xlsx

B: monthly_backup.ps1

C: mails.zip

D: to_do_list_final_v2.txt

DIE

NTS DEFENSE

QUIZ-SHOW

50/50

€ 4.000

Welche Datei soll unser Angreifer nun genauer betrachten?

A: passwords.xlsx

B: monthly_backup.ps1

C: mails.zip

D: to_do_list_final_v2.txt

INTRUSION DETECTION HONEY POT

Honeypots und **Honeynets** sind Computersysteme oder Netzwerkkomponenten, die gezielt Angreifer anlocken sollen

INTRUSION DETECTION HONEY POT

- Einmaliger geringer Aufwand mit großem Gewinn
- Bestens auf die Kundenumgebung (verwendeter Username und eingesetzte Software-Service) angepasst
- Lenken Angreifer vom realen Produktionsnetzwerk ab
- Niedrige False-Positive Rate
- Kaum Wartung
- Geringe Logging-Kapazität / Logvolumen

BLOCK DES ANGRIFFS

- Der Analyst hat nun die Überhand
- Er hat ein klares Bild über den Angriff, den Einstiegsvektor sowie die Ausmaße und entscheidet sich den Angriff nun endgültig zu blocken
- Dank EDR können Angriffe blockiert, Endpunkte isoliert und weitere Endgeräte überprüft werden

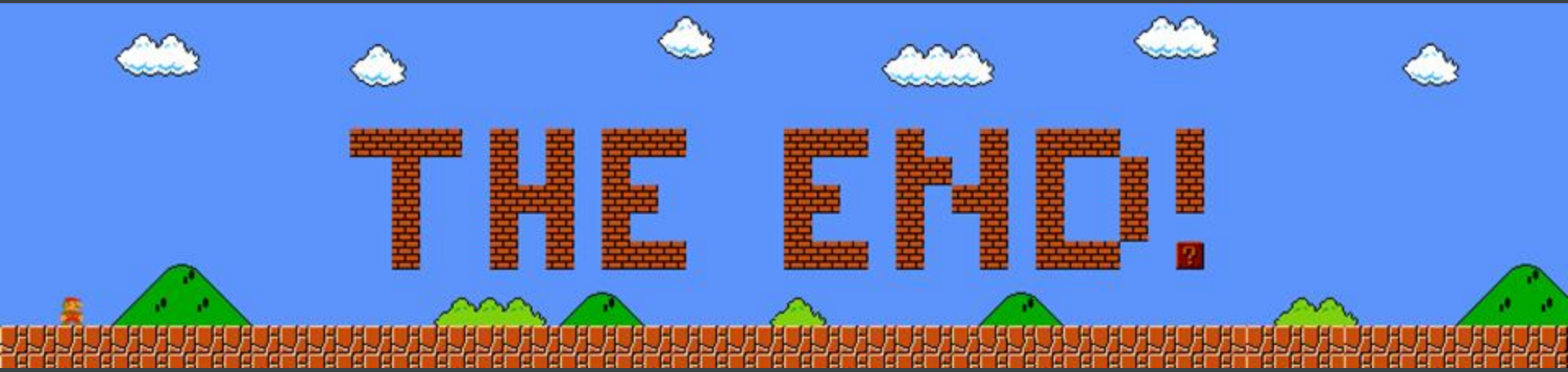
HERAUSFORDERUNGEN

- Langsames Vorgehen des Angreifers (Rauschen der Logs)
- Service und Use Cases sollten bestmöglich an die Kundenumgebung sowie dessen Kerngeschäfte angepasst werden
- Schwierig Sicherheitsexperten zu finden
- Budget und Zeit für die Implementierung + den Betrieb eines solchen Services

NTS

POST MORTEM

- Werden E-Mails von Externen gekennzeichnet?
- Können weitere Dateitypen geblockt werden?
- Hätte man das das Verhalten des Nutzers vielleicht durch Security Awareness Schulungen verhindern können?
- Wurden Security Mail Appliances eingesetzt? (z.B. Cisco ESA)
- Existieren DMARC Records um Spoofing vorzubeugen?


THE END!