T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Berlin, 14. - 15.11.2017

E-Mail-Sicherheit

Stefan Cink, Net at Work

Wer wir sind

Net at Work entwickelt das innovative Secure E-Mail-Gateway NoSpamProxy für einen umfassenden **Schutz vor Spam und Malware** und zur **Verschlüsselung**. NoSpamProxy läuft auf **Windows Server** und schützt zuverlässig im Hintergrund.

Aus der Erfahrung als Anwender und aus vielen Projekten sind Installation, Konfiguration und Betrieb praxisorientiert und besonders einfach.

Gründung
1995
Mitarbeiter
>60
Standort
Paderborn
Kompetenz
msxfaq.de
informiert
ca. 6000
Admins
täglich

Zertifizierungen/Partner:

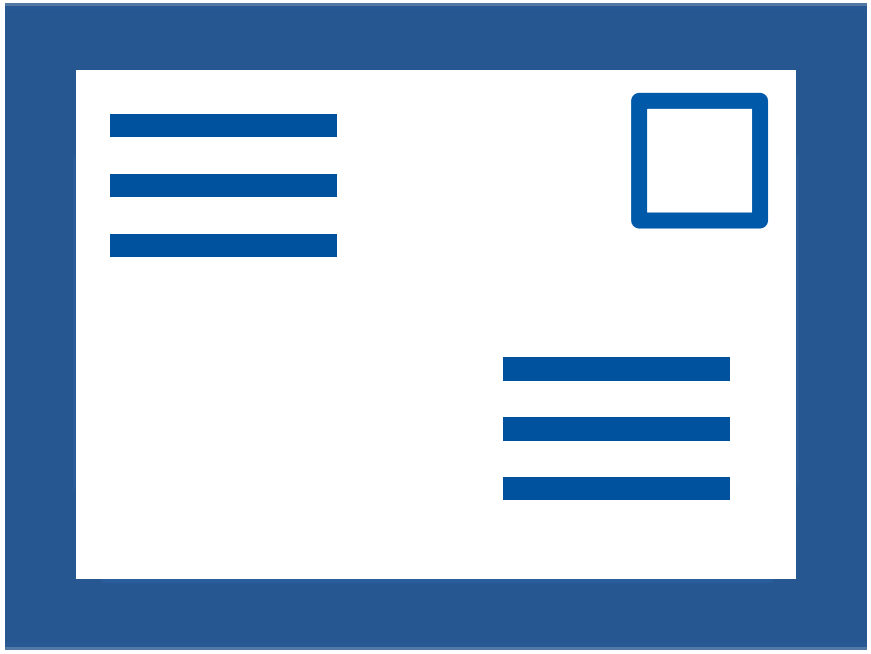
Microsoft Partner
Gold Messaging
Gold Communications
Gold Collaboration and Content
Gold Cloud Productivity
Gold Application Development

SecurITy made in Germany

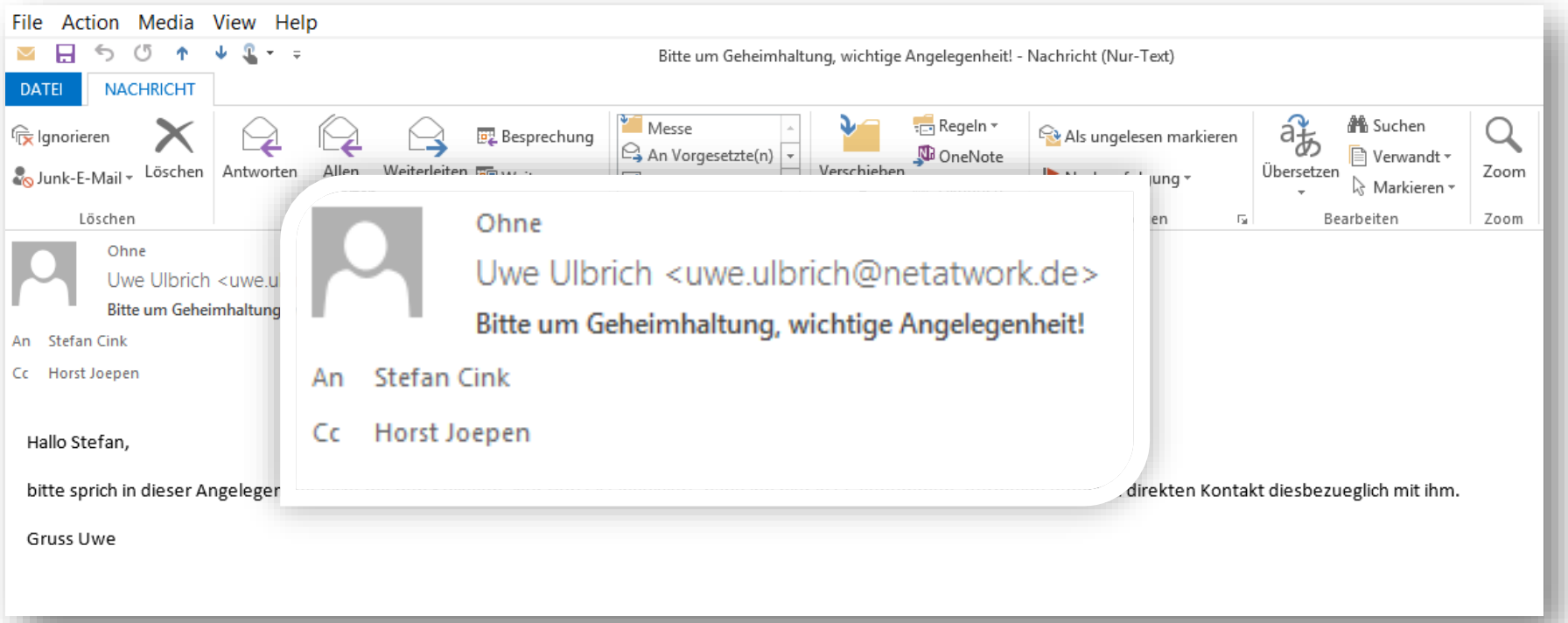
Windows Server 2012 R2 Certified

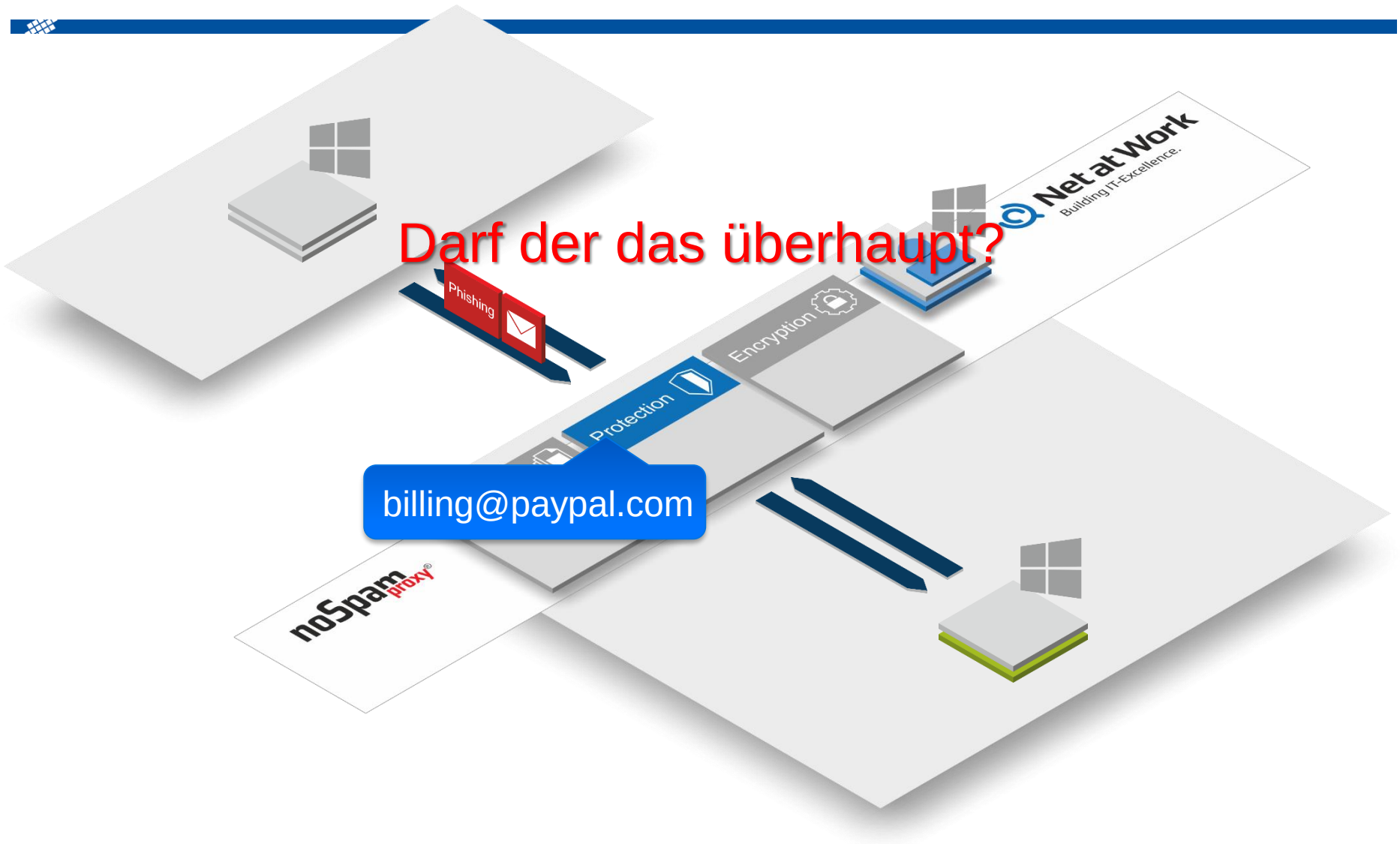
Absenderreputation

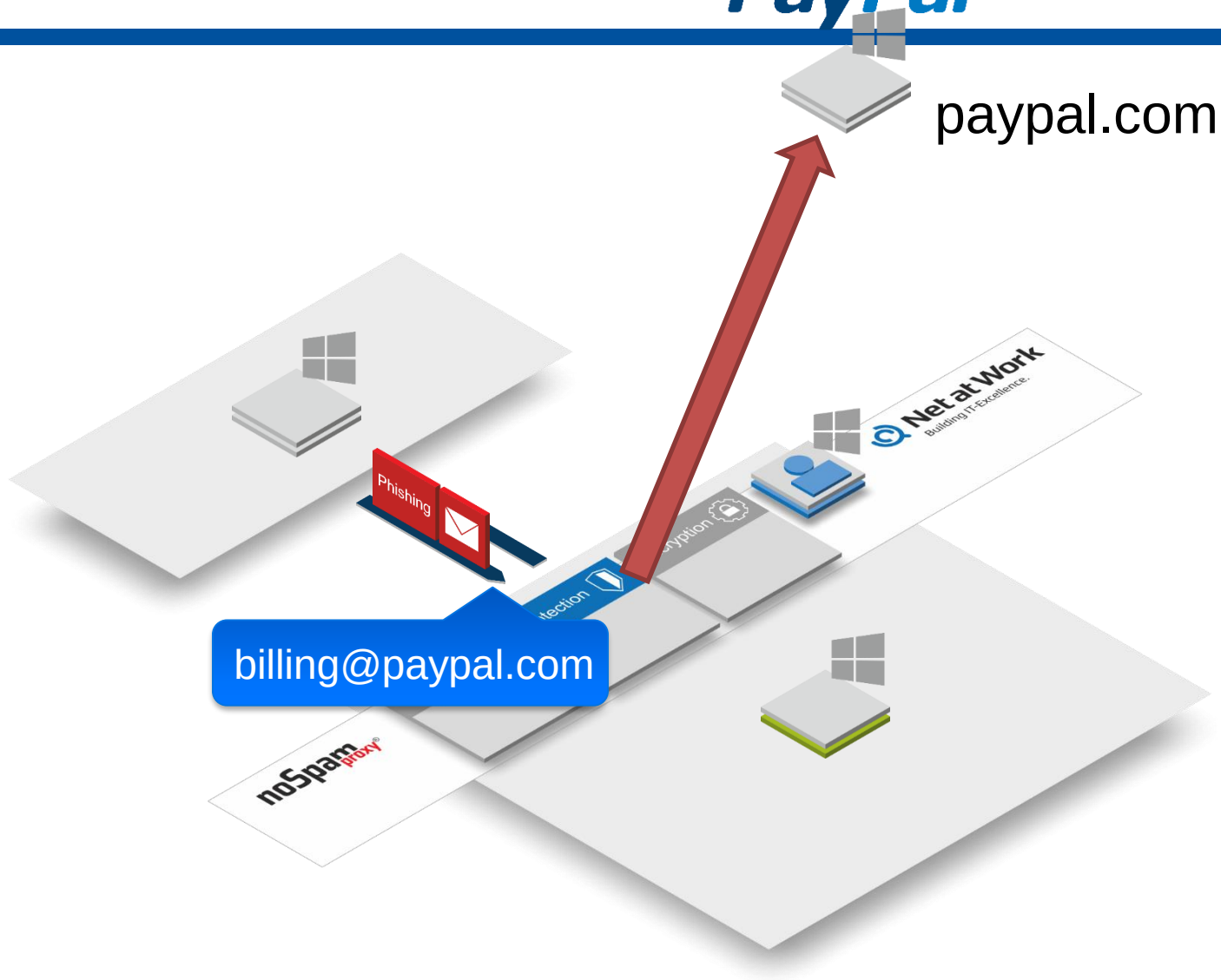
Envelope Sender vs. Body from



Envelope Sender vs. Body from




Darf der das überhaupt?
Phishing
Encryption
Protection
billing@paypal.com
noSpam proxy
Net at Work
Building IT-Excellence.

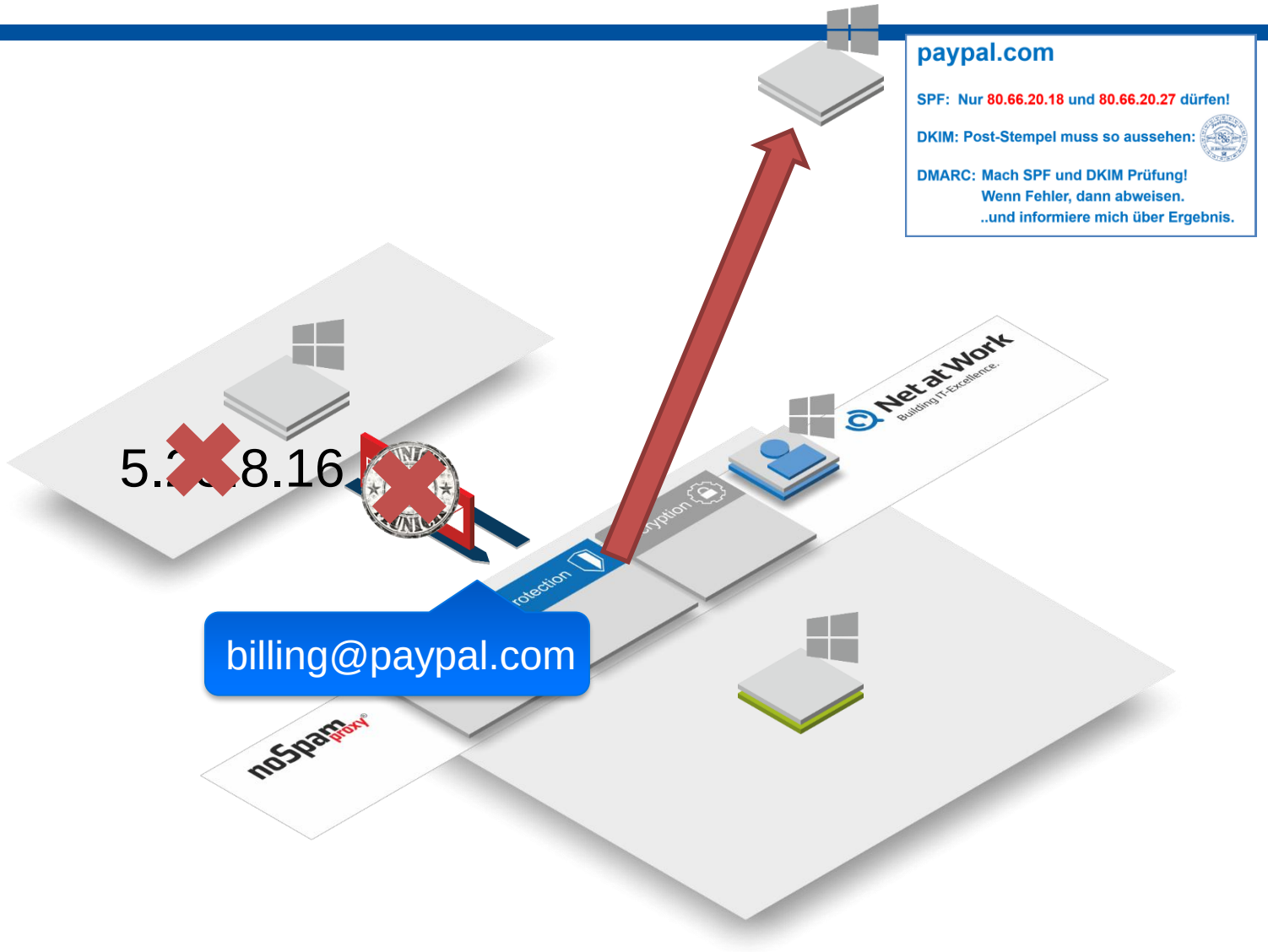

paypal.com
Phishing
billing@paypal.com
Net at Work
Building IT-Excellence.
noSpam proxy

paypal.com

SPF: Nur 80.66.20.18 und 80.66.20.27 dürfen!

DKIM: Post-Stempel muss so aussehen:

DMARC: Mach SPF und DKIM Prüfung!
Wenn Fehler, dann abweisen.
..und informiere mich über Ergebnis.


paypal.com
SPF: Nur 80.66.20.18 und 80.66.20.27 dürfen!
DKIM: Post-Stempel muss so aussehen:
DMARC: Mach SPF und DKIM Prüfung!
Wenn Fehler, dann abweisen.
..und informiere mich über Ergebnis.
billing@paypal.com
Net at Work
Building IT-Excellence.
noSpam proxy

Unter der Motorhaube

Sender Policy Framework (SPF)

netatwork.de

A	www.netatwork.de	80.66.20.21
A	mail.netatwork.de	80.66.20.22
MX	netatwork.de	mail.netatwork.de
TXT	netatwork.de	v=spf1 +MX -All

Domain Key Identified Mail (DKIM)

netatwork.de

A	www.netatwork.de	80.66.20.21
A	mail.netatwork.de	80.66.20.22
MX	netatwork.de	mail.netatwork.de
TXT	netatwork.de	v=spf1 +MX -All
TXT	selektor._domainkey.netatwork.de	v=DKIM1; p=123; s=email

Absenderreputation

Domain-based Message Authentication, Reporting and Conformance (DMARC)

```
v=DMARC1;
        p=none;
        rua=mailto:dmarc_rua@netatwork.de;
        ruf=mailto:dmarc_ruf@netatwork.de;
        fo=1;
        adkim=s;
        aspf=s;
        rf=afrf;
        sp=none
```

Weitere Vorteile von DMARC

- **Sender Alignment: Envelope Sender = Body from**
- **Weniger Missbrauch: Ed Tucker vom HMRC*: 500 Mio. Spam-Mails p.a. weniger!**
- **Senkung des Reputations-Risikos**
- **"Weiterleitungs-Problem" i.d.R. gefixt**

* https://hmrcdigital.blog.gov.uk/2016/11/25/combatting-phishing-a-very-big-milestone/

Weitere Vorteile von DMARC

fraudmarc

Netflix's use of DMARC reduced damage from huge email scam

DMARC

You may be aware that, last Friday, scammers sent out a phishing email to up to 110 million Netflix subscribers. The email included a link to a fake Netflix website that asked users to login and enter their credit card information.

However, a clear indication of a scam can be found higher up on this message: there is NO SENDER!

Fortunately for Netflix customers (and unfortunately for the scammers), Netflix is responsible when it comes to email security. The scammers couldn't claim to send from netflix.com because Netflix uses a security policy called DMARC to protect its domain against phishing attacks.

* https://www.fraudmarc.com/netflix-uses-dmarc-to-protect-customers/

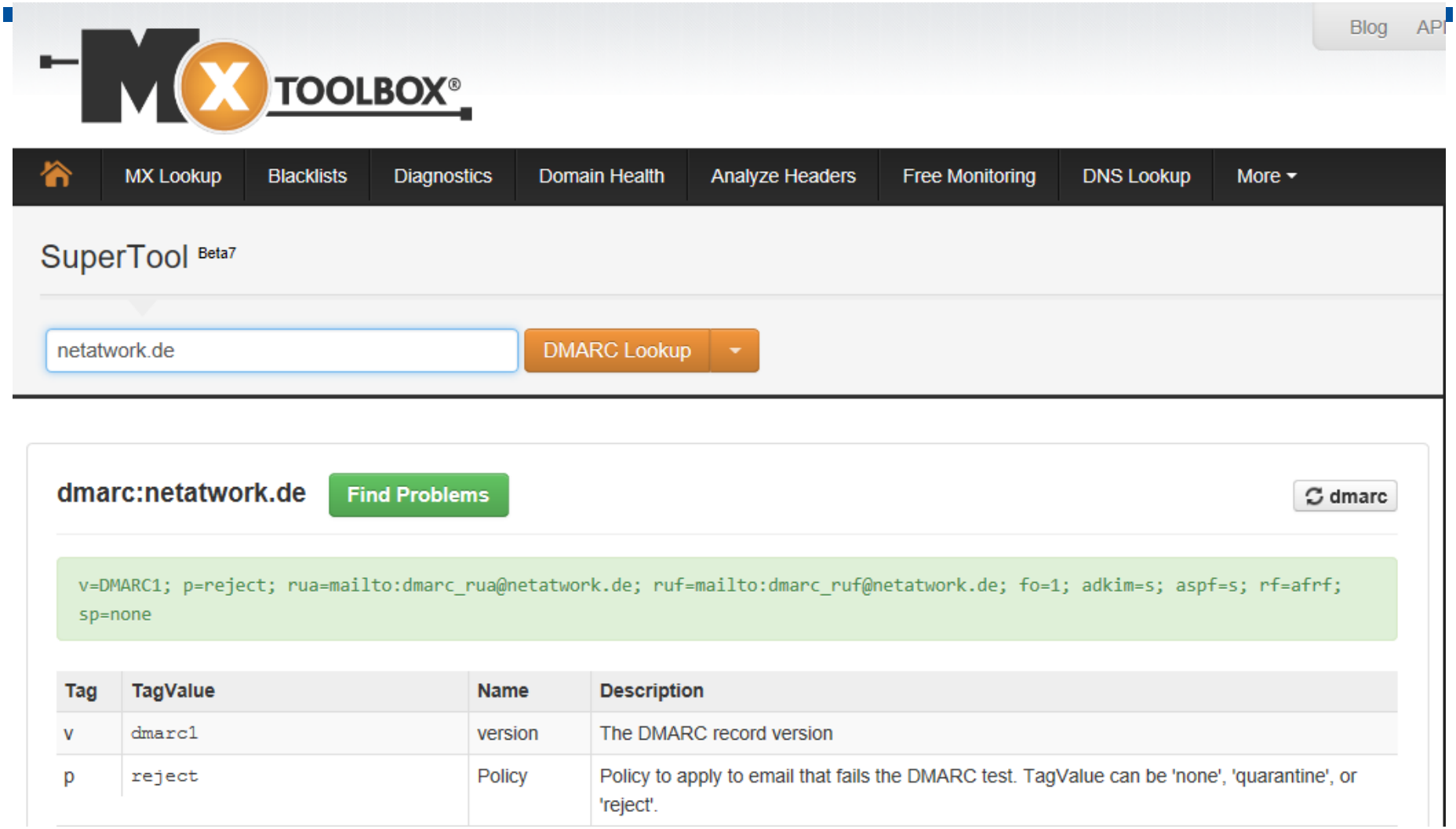
Received: from LEJPR01MB0170.DEUPRD01.PROD.OUTLOOK.DE (10.158.141.9) by LEXPR01MB0176.DEUPRD01.PROD.OUTLOOK.DE (10.158.164.13) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1157.12 via Mailbox Transport; Wed, 21 Jun 2017 08:38:51 +0000
Received: from FRXPR01CA0072.DEUPRD01.PROD.OUTLOOK.DE (2a01:4180:c010:15::40) by LEJPR01MB0170.DEUPRD01.PROD.OUTLOOK.DE (2a01:4180:c012:6::9) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1178.14; Wed, 21 Jun 2017 08:38:50 +0000
Received: from LEJGER01FT003.eop-ger01.prod.protection.outlook.de (2a01:4180:4051:800::202) by FRXPR01CA0072.outlook.office.de (2a01:4180:c010:15::40) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1199.15 via [redacted]
Authentication-Results: spf=softfail (sender IP is 52.178.24.80) smtp.mailfrom=paypal.de; joepen-itconsult.com; dkim=none (message not signed) header.d=none;joepen-itconsult.com; dmarc=fail action=oreject
[redacted]
Received-SPF: SoftFail (protection.outlook.com: domain of transitioning paypal.de discourages use of 52.178.24.80 as permitted sender)
Received: from bla.de (52.178.24.80) by LEJGER01FT003.mail.protection.outlook.de (10.157.128.88) with Microsoft SMTP Server id 15.1.1178.19 via Frontend Transport; Wed, 21 Jun 2017 08:38:50 +0000
From: Paypal SE <info@paypal.de>
Date: Wed, 21 Jun 2017 10:38:50 +0200
Subject: Datendiebstahl bei Paypal, Sie sind ebenfalls betroffen!
Message-ID: <GJLKBU6FM1U4.Q0W94X6WGTC83@nspcink001>
To: <horst.joepen@joepen-itconsult.com>
MIME-Version: 1.0
Content-Type: text/html; charset="utf-8"
Content-ID: <Z9TNBU6FM1U4.851DQF74L9JI2@nspcink001>
Return-Path: info@paypal.de

Wie pack ich‘s an?

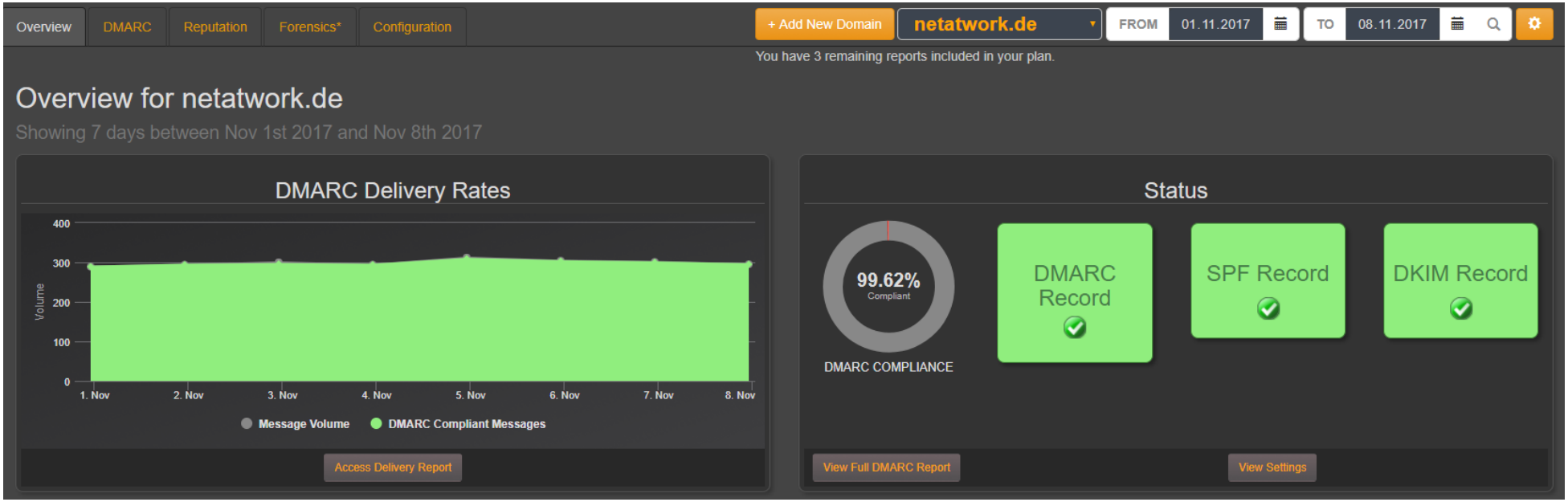
Wie pack ich‘s an?

Source IP	Company	Count	DMARC - SPF	Header From	SPF Domain	SPF Result
80.66.20.18	netatwork	78749	pass	netatwork.de	netatwork.de	pass
194.126.158.98	inet-service	746	fail	netatwork.de	inet-service.com	pass
81.7.3.168	huestel	51	fail	email.netatwork.de	huestel.de	none
151.189.21.127	arcor-online	47	fail	netatwork.de	netatwork.de	fail
86.110.75.249	smtp-gateway	42	fail	netatwork.de	inet-service.com	fail
131.234.142.9	uni-paderborn	29	fail	netatwork.de	netatwork.de	fail
212.227.126.135	kundenserver	23	fail	netatwork.de	srs2.kundenserver.de	pass
2a01:488:42:1000:b24d:6de0::	sendnode	22	fail	neu.netatwork.de	nospamproxy.de	neutral
207.46.100.93	outlook	19	pass	Netatwork.de	netatwork.de	pass
46.50.224.123	zsttk	16	fail	netatwork.de	zsttk.net	none

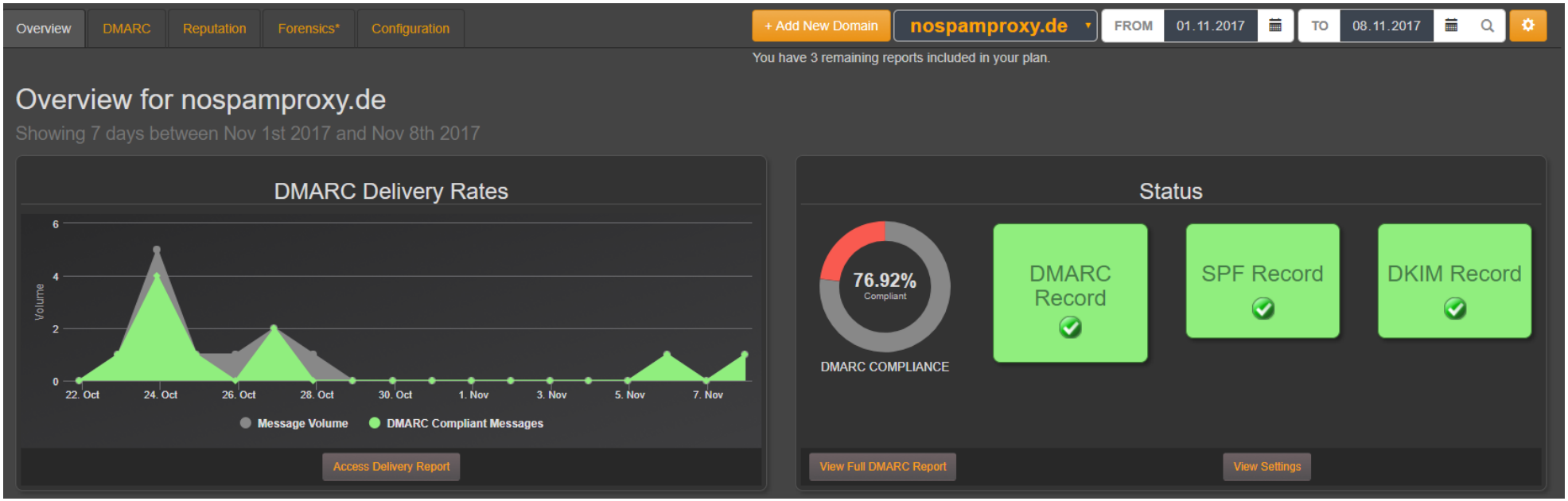
Welche Tools gibt es?



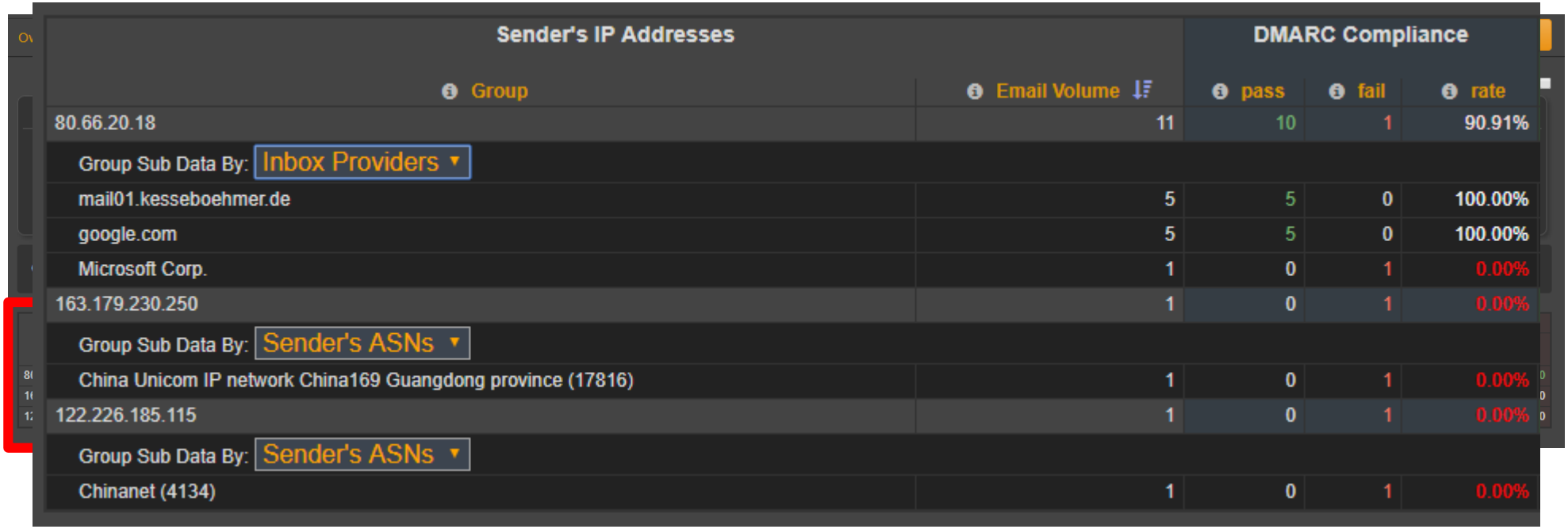
Welche Tools gibt es?



Welche Tools gibt es?



Welche Tools gibt es?



Sender's IP Addresses		DMARC Compliance		
Group	Email Volume	pass	fail	rate
80.66.20.18	11	10	1	90.91%
Group Sub Data By: Inbox Providers				
mail01.kesseboehmer.de	5	5	0	100.00%
google.com	5	5	0	100.00%
Microsoft Corp.	1	0	1	0.00%
163.179.230.250	1	0	1	0.00%
Group Sub Data By: Sender's ASNs				
China Unicom IP network China169 Guangdong province (17816)	1	0	1	0.00%
122.226.185.115	1	0	1	0.00%
Group Sub Data By: Sender's ASNs				
Chinanet (4134)	1	0	1	0.00%

Und was ist mit CEO Scam?

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL Plus | Abo | Shop Schlagzeilen | Wetter | TV-Programm | mehr ▼

Login | Registrierung

SPIEGEL ONLINE **WIRTSCHAFT**

Suche Kurse

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

Nachrichten > Wirtschaft > Unternehmen & Märkte > Trickbetrug > Leoni AG: Betrüger prellen Leoni um 40 Millionen Euro

Geldanlage

Autozulieferer: Betrüger prellen Leoni um 40 Millionen Euro

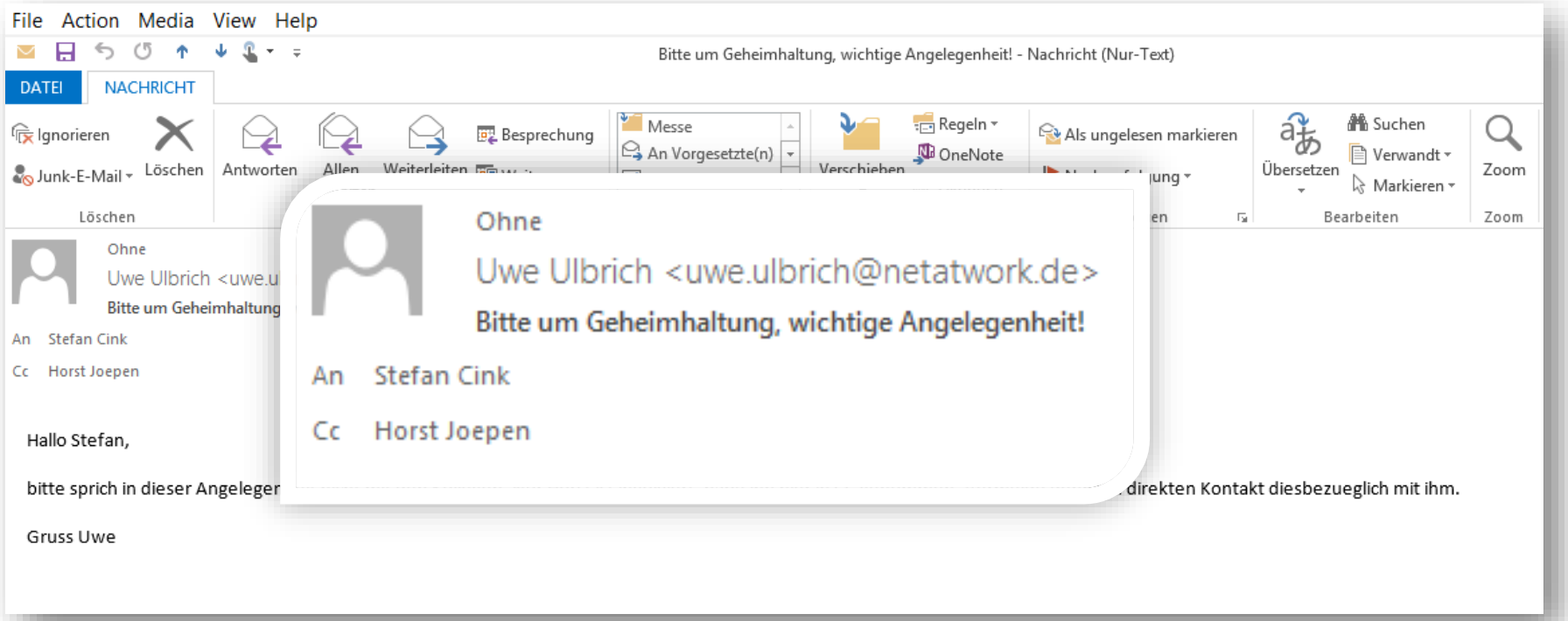
DPA

Leoni-Sitz in Nürnberg (Archivfoto)

Der Autozulieferer Leoni ist nach eigenen Angaben Opfer eines millionenschweren Betrugs geworden. Die Täter seien besonders raffiniert vorgegangen und hätten gefälschte Dokumente und Identitäten benutzt.

Was war passiert?

Die Darstellung im E-Mail-Client



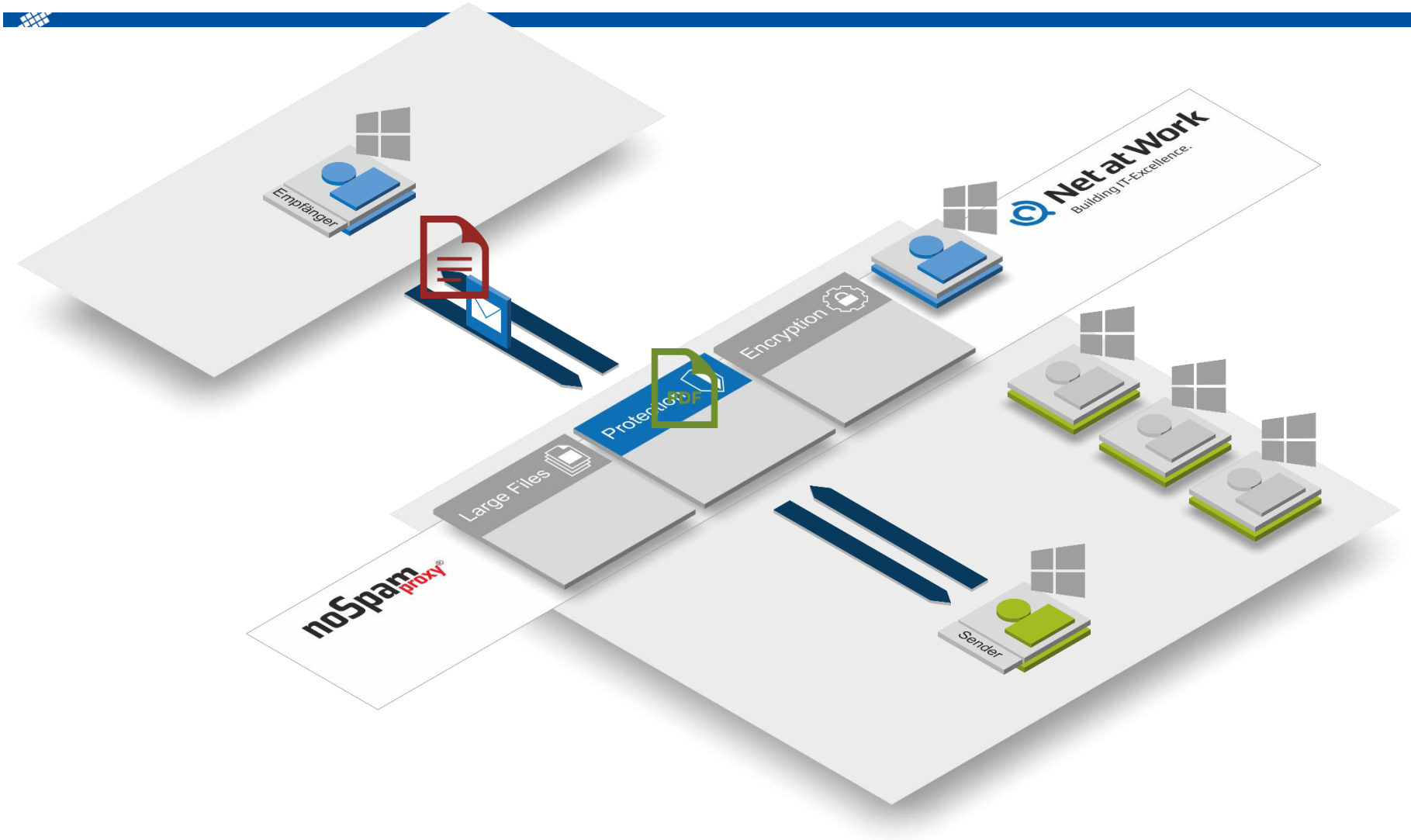
Die Lösung

- Synchronisation mit Active Directory, inkl. vollständigen Namen
- Umfangreiche Prüfung der Absenderangaben auch im Header!
- Miteinander sprechen!

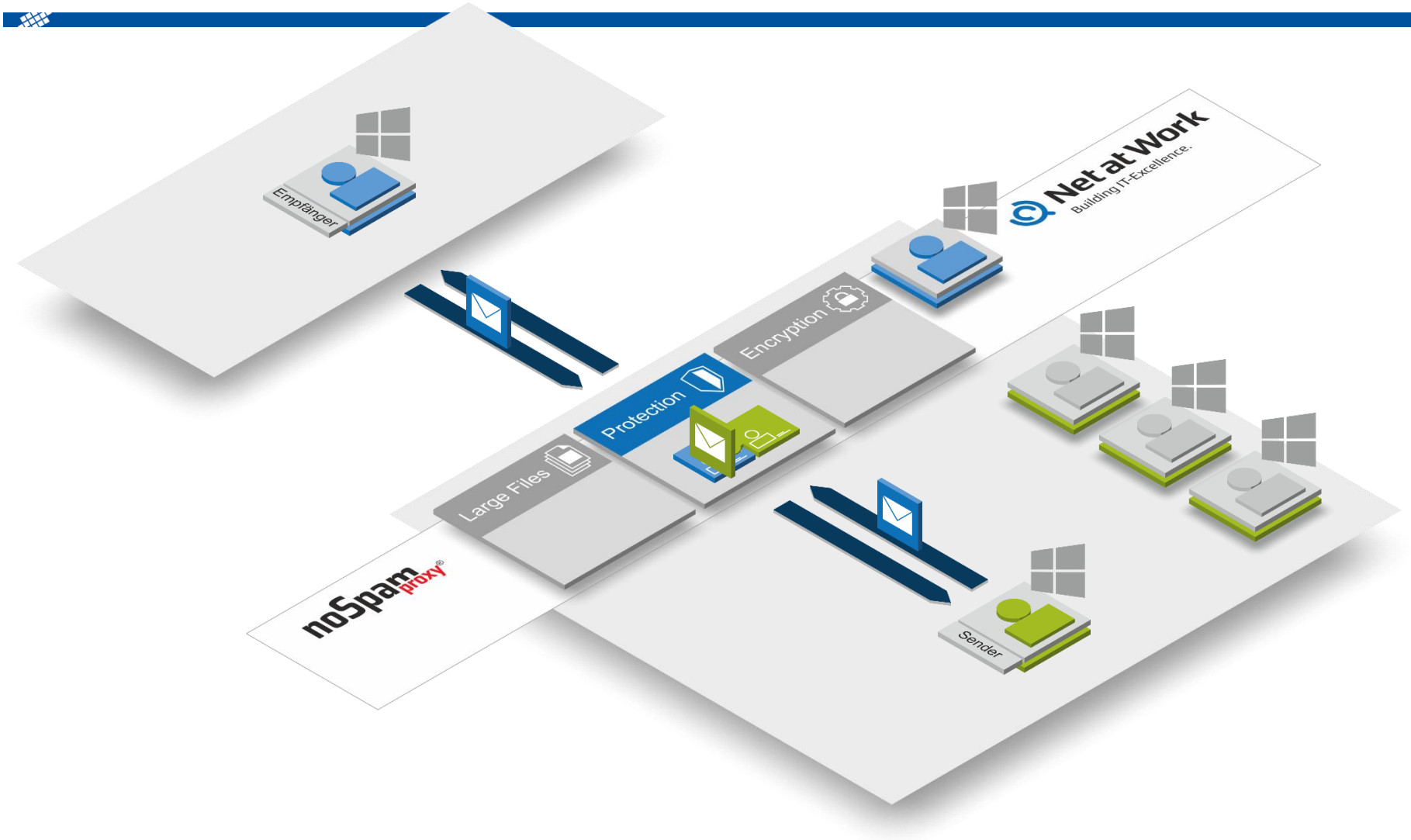
Die größte Sicherheitslücke hat immer einen Vor- und Nachnamen

Ein Röntgenbild?

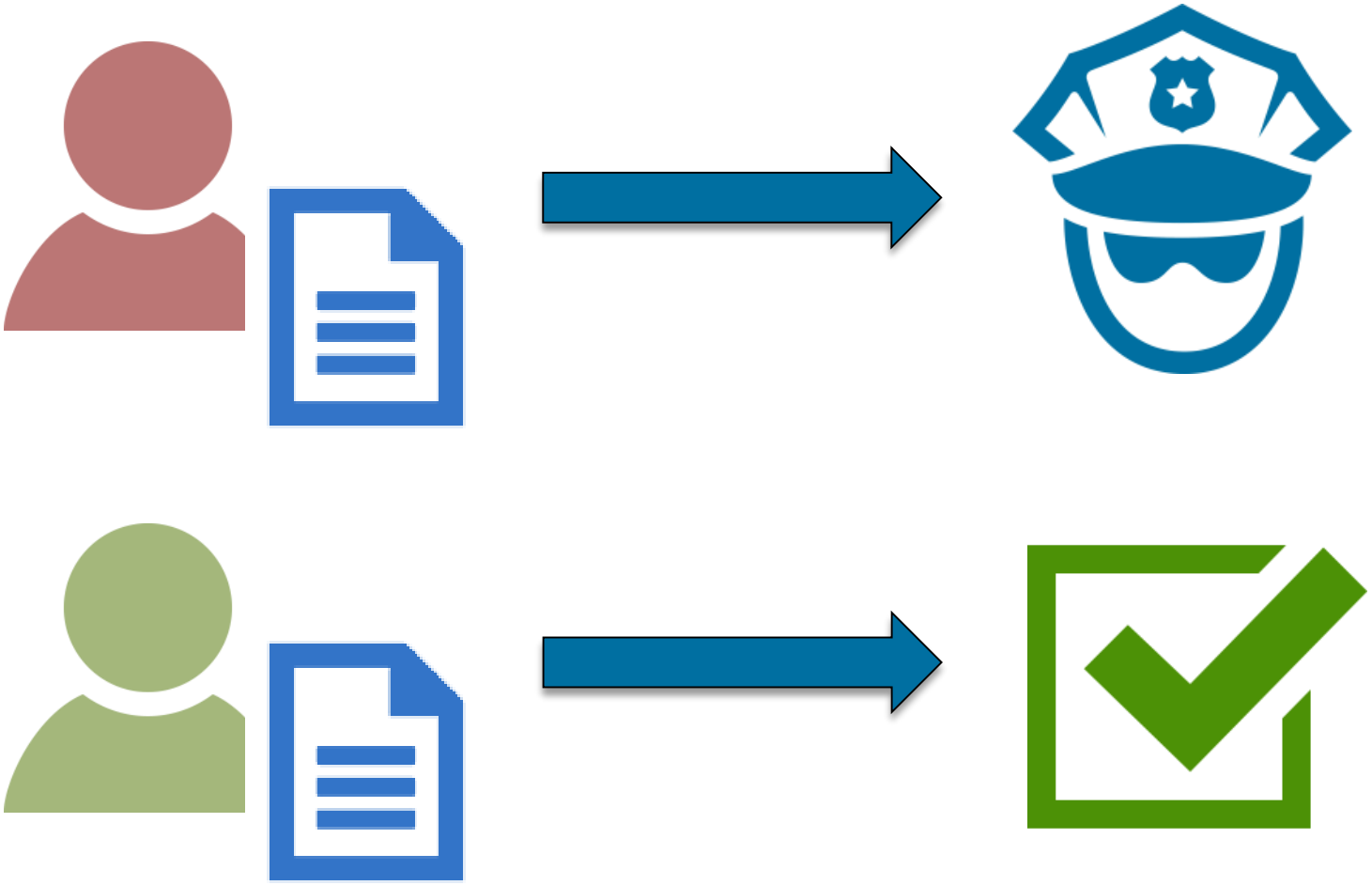
Ein Röntgenbild?



Level of Trust



Level of Trust und Anhangsmanagement



Vielen Dank!