Praktische Maßnahmen zur Cybersicherheit von Binnenschifffahrtsunternehmen

Bernd Dettmers
net.e – Network Experts GmbH

Bernd Dettmers

net.e - Network Experts GmbH

- Allianz für Cybersicherheit
- HackerOne
- Chaos Computer Club
- OSCP (Offensive Security Certified Professional)
- Arbeitskreis Cyber Security Awareness Maritime Wirtschaft (MCN)

Schwachstellenanalyse

Penetrationstests
Codeanalyse
IT-Audits

Netzwerktechnik

Konzeptionierung
Analyse
Umstrukturierung

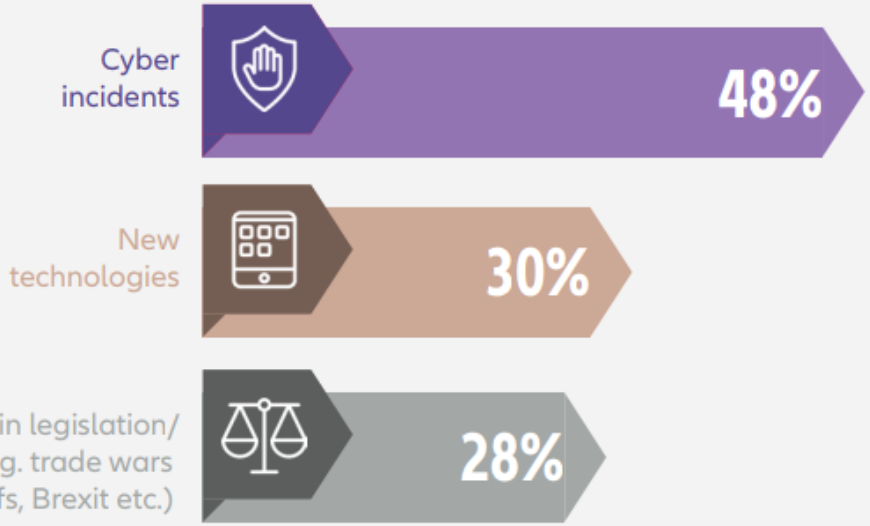
Security Awareness

Live Hacking
Phishing
Workshops

IT-Forensik

Datenrettung
Angriffsanalyse
Ermittlung

WHAT ARE THE TOP EMERGING BUSINESS RISKS FOR THE NEXT THREE TO FIVE YEARS?



Source: Allianz Global Corporate & Specialty.
Figures represent the percentage of answers of all participants who responded (2,415). Figures don't add up to 100% as up to three risks could be selected.

Welche Motive und Absichten verfolgen die Angreifer?

Kriminelle Energie

Datendiebstahl:
jeder Datensatz bringt Geld

Racheakt

Ehemalige Mitarbeiter als
Innentäter

Spionage

Verschaffen eines
Wettbewerbvorteils

Vertuschung von Straftaten

Missbräuchliche
Servernutzung

Servernutzung für illegale Zwecke

Illegale Spielepartys

Hacken als Volkssport

IT-Szeneprofilierung

Wie gehen Hacker vor?

Anatomie eines Cyberangriffes

Aufklärung/ Erkundung	Zugriff verschaffen	Eindringen/ Penetration/	Festsetzung für eine lange Persistenz	Ausschleusen von Daten	„Sanierung“
Sammeln detaillierter Informationen über das Unternehmen und pot. Ziele	Ausmachen einer Sicherheitslücke im Unternehmen (häufig über eine Phishing-Mail)	Eindringen in das Unternehmens-netzwerk um ihren Zugriff auszuweiten	Installation getarnter Dienste zur weiteren Ausnutzung von Schwachstellen	Verschlüsseln der Daten, um sie unbemerkt aus dem Netzwerk zu schleusen	Verwischen des Fremdzugriffs / Saubere Flucht

Angriffsziel Binnenschifffahrt

- Ransomware
- CEO Fraud / Phishing
- USB Sticks

We can confirm that Maersk IT systems are down across multiple sites and business unit due to a cyber attack. We continue to assess the situation. The safety of our employees, our operations and customers business is our top priority. We will update when we have more information.

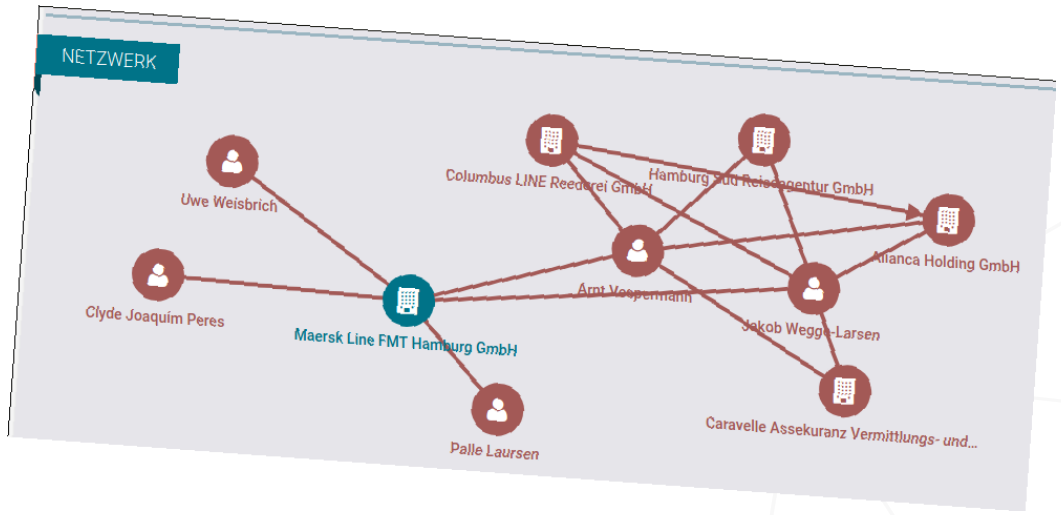
Ransomware

- MAERSK
- Deutsche Post
- Honda
- MERCK
- Deutsche Bahn
- Mondelez
- Beiersdorf
- Ukraine

Wie gehen Hacker vor?

Information Gathering

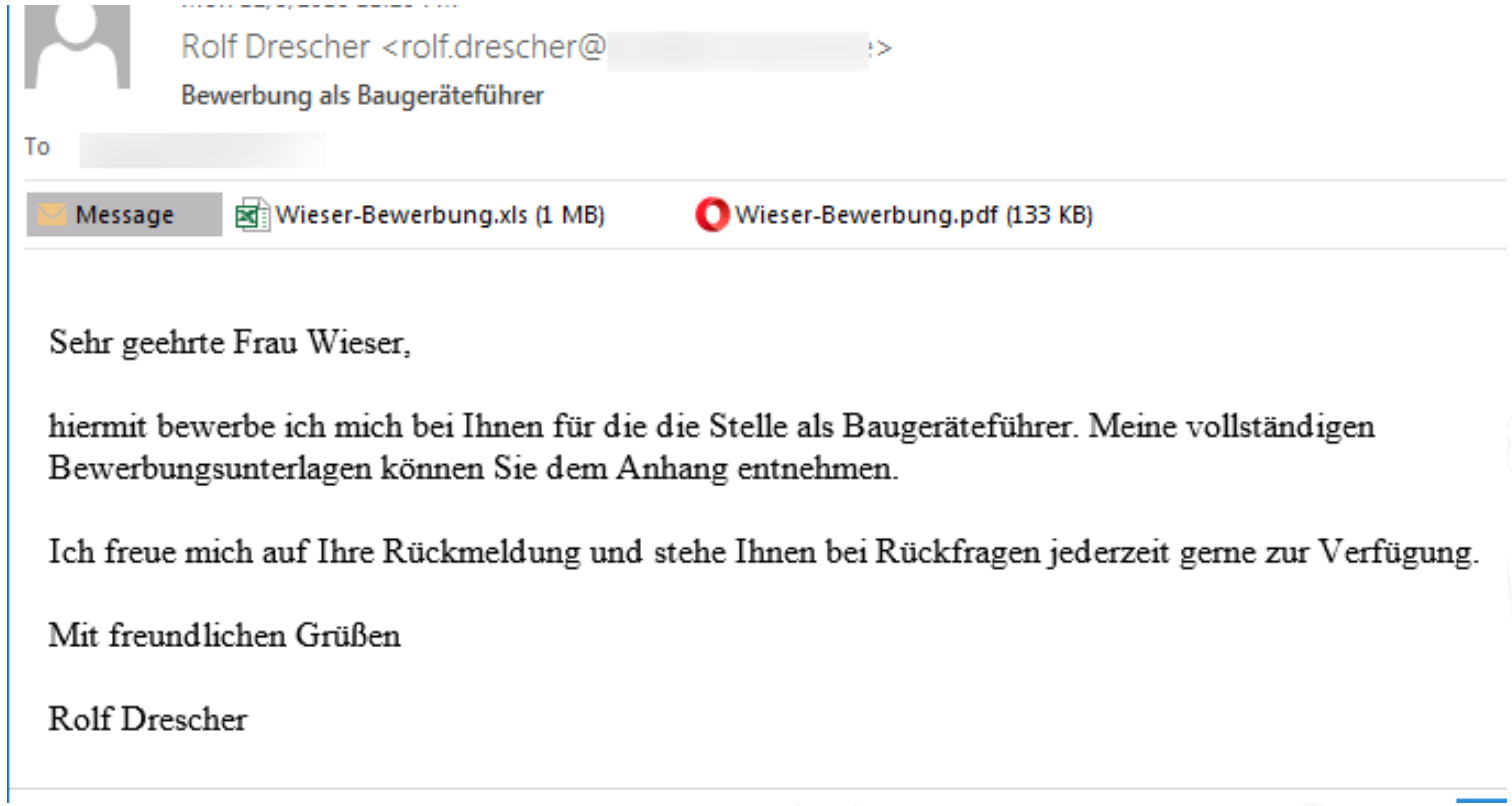
- Stellenausschreibungen
- Mit wem arbeiten Sie zusammen?



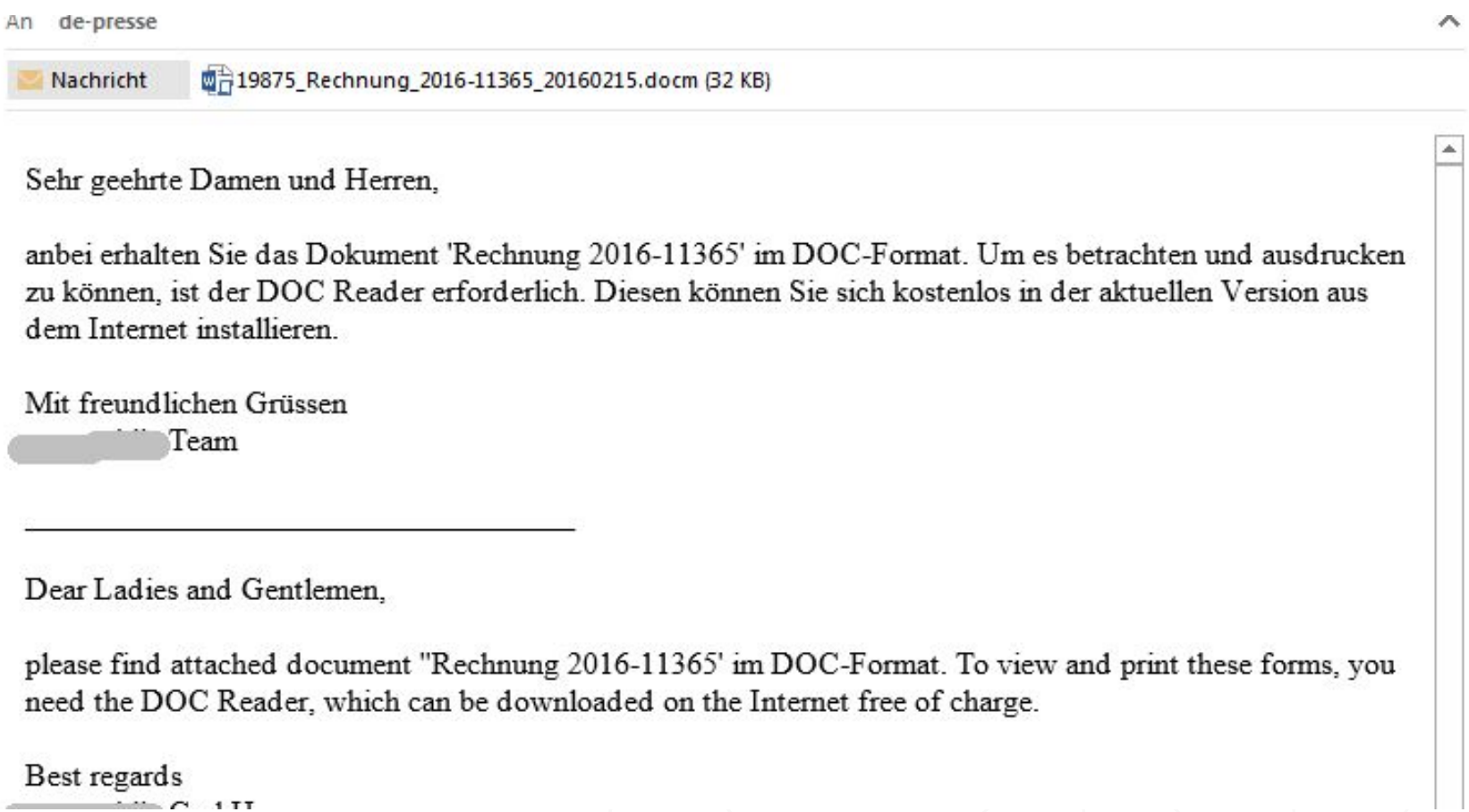
MAERSK

		OUR SOLUTIONS	ABOUT MAERSK	GLOBAL PRESENCE	LOCAL INFORMATION
8/26/2019	Sales support	Commercial/Sales/Business Development			Pakistan
8/26/2019	Workstream Lead	Project/Process/Performance Management			Singapore
8/26/2019	Care Business Partner - Reefer	Customer Service			South Africa
8/26/2019	Analyst AR	Finance/Accounting			India
8/26/2019	Copy of #61318867 Technical Specialist 02	IT			India
8/26/2019	Korean Speaker Team Leader	Commercial/Sales/Business Development			China
8/26/2019	L&S Business Development Partner-PRS	Commercial/Sales/Business Development			China
8/25/2019	Sales Executive -Trade Finance	Commercial/Sales/Business Development			India

Ransomware?!


Rolf Drescher <rolf.drescher@
Bewerbung als Baugeräteführer
To
Message
Wieser-Bewerbung.xls (1 MB)
Wieser-Bewerbung.pdf (133 KB)
Sehr geehrte Frau Wieser,
hiermit bewerbe ich mich bei Ihnen für die die Stelle als Baugeräteführer. 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

Ransomware?!



An de-presse

Nachricht 19875_Rechnung_2016-11365_20160215.docm (32 KB)

Sehr geehrte Damen und Herren,

anbei erhalten Sie das Dokument 'Rechnung 2016-11365' im DOC-Format. Um es betrachten und ausdrucken zu können, ist der DOC Reader erforderlich. Diesen können Sie sich kostenlos in der aktuellen Version aus dem Internet installieren.

Mit freundlichen Grüssen
[redacted] Team

Dear Ladies and Gentlemen,

please find attached document "Rechnung 2016-11365' im DOC-Format. To view and print these forms, you need the DOC Reader, which can be downloaded on the Internet free of charge.

Best regards

Ransomware?!

Gegenmaßnahmen

- Backup Strategien
- Netzwerksegmentierung
- Aktuelle Systeme
- Aktuelle Virensignaturen
- Regelmäßige Awareness-Maßnahmen (Schulungen, Phishing)

CEO Fraud?

CEO Fraud

CEO-FRAUD

Google und Facebook um 100 Millionen US-Dollar betrogen

CEO-FRAUD

Autozulieferer Leoni um 40 Millionen Euro betrogen

Mitarbeiterin sollte Geld überweisen

Banküberweisung nach London: Betrüger ergaunerten 49.000 Euro

26.01.18 - 16:31

20.02.2018, PP Oberbayern Süd

Betrugsmasche „CEO-Fraud“: Firma überweist fast 70.000 Euro

Wie gehen Hacker vor?

CEO Fraud

Sehr geehrter [redacted]

zurzeit bereiten wir die Übernahme eines Unternehmens vor, welches insbesondere die erforderlichen finanziellen Transaktionen erfordert.

Diese Angelegenheit muss absolut vertraulich behandelt werden, weshalb Niemand sonst, auch nicht innerhalb unseres Hauses, bis zur öffentlichen Bekanntmachung darüber informiert wird.
Diese Bekanntmachung des Übernahmeangebots erfolgt in Kürze. Respektive nach Abwicklung der Übernahme.
Aufgrund Ihrer Diskretion und Ihrer bisher einwandfreien Arbeit in unserem Unternehmen möchte ich Ihnen die Verantwortung für dieses Projekt übertragen.
Da die gesamte Transaktion absolut vertraulich behandelt werden muss, bitte ich Sie, den Stand der Transaktion nur mit mir ausnahmslos per E-Mail abzustimmen.
Diese Angelegenheit darf und muss ausnahmslos nur mit Ihnen, [redacted] von der [redacted] zunächst unsere Bankverbindung für die weitere Bearbeitung zu übermitteln und mir erörtert werden.
Weiter bitte ich Sie, mich in dieser Angelegenheit weder persönlich noch telefonisch zu kontaktieren. Jede Erörterung der geplanten Übernahme erfolgt ausnahmslos per E-Mail an Sie oder mich, auch um eine ausreichende Dokumentation gemäß den FMA Richtlinien sicherzustellen.
Können wir mit heutigem Wertstellungsdatum eine Zahlung im Außenwirtschaftsverkehr vornehmen ohne irgendwelche Fragen aufzuwerfen?

Mit freundlichen Grüßen

Rechnungsfälschung

EUR	**43.500,00**

Free of tax according to §4, no. 2 in connection with §8, no. 1 UstG.
Our VAT Reg No DE 814 105 968 Your VAT Reg No 101633
Our Tax 60/220/19900

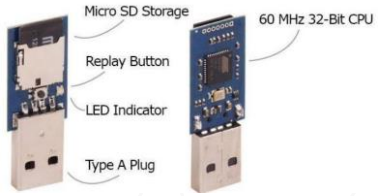
CEO Fraud?!

Gegenmaßnahmen

- Achtsam sein
- Bei ungewöhnlichen Zahlungsanweisungen, immer den E-Mail Absender überprüfen und mit dem Vorgesetzten Kontakt aufnehmen
- Regelmäßige Awareness-Maßnahmen (Schulungen, Phishing)

USB Sticks

- Bad USB
- Rubber Ducky
- LAN Turtle
- USB Ninja



The Washington Post
Democracy Dies in Darkness

National Security

Chinese woman carrying thumb drive with malware arrested at Trump's Mar-a-Lago resort

By **Devlin Barrett** and **David A. Fahrenthold**
April 2

Secret Service agents arrested a Chinese woman after she bypassed layers of security and gained access to the reception area of President Trump's Florida resort this past weekend, saying they found she was carrying two passports and a thumb drive containing malicious software, according to court documents.

USB Sticks

Gegenmaßnahmen

- Quarantäne Rechner
- USB Ladekabel nicht an den Rechner anschließen
- USB Ports sperren (Software und Physisch)
- Regelmäßige Awareness-Maßnahmen (Schulungen, Phishing)

net.e
NETWORK EXPERTS

Mit Sicherheit zum Erfolg!

net.e – Network Experts GmbH

Tel. 04941/7399760 | b.dettmers@net-e.de

www.net-e.de