Florian Jörgens

Hacked!
72 hours of a CISO's nightmare

A tabletop exercise

Florian Jörgens

Chief Information Security Officer, Vorwerk

- PricewaterhouseCoopers, IT-Auditor, 2013 - 2016
- E.ON, Information Security Manager, 2016 - 2019
- LANXESS, CISO, 2019 - 2021
- FOM, Lecturer, research assistant, since 2015
- HS Fresenius, Lecturer, since 2017

Procedure

01

02

03

Round 01

Round 02

Round 03

At the end of each round, there are different possible actions that can be named by a show of hands.

Introduction

INTRODUCTION

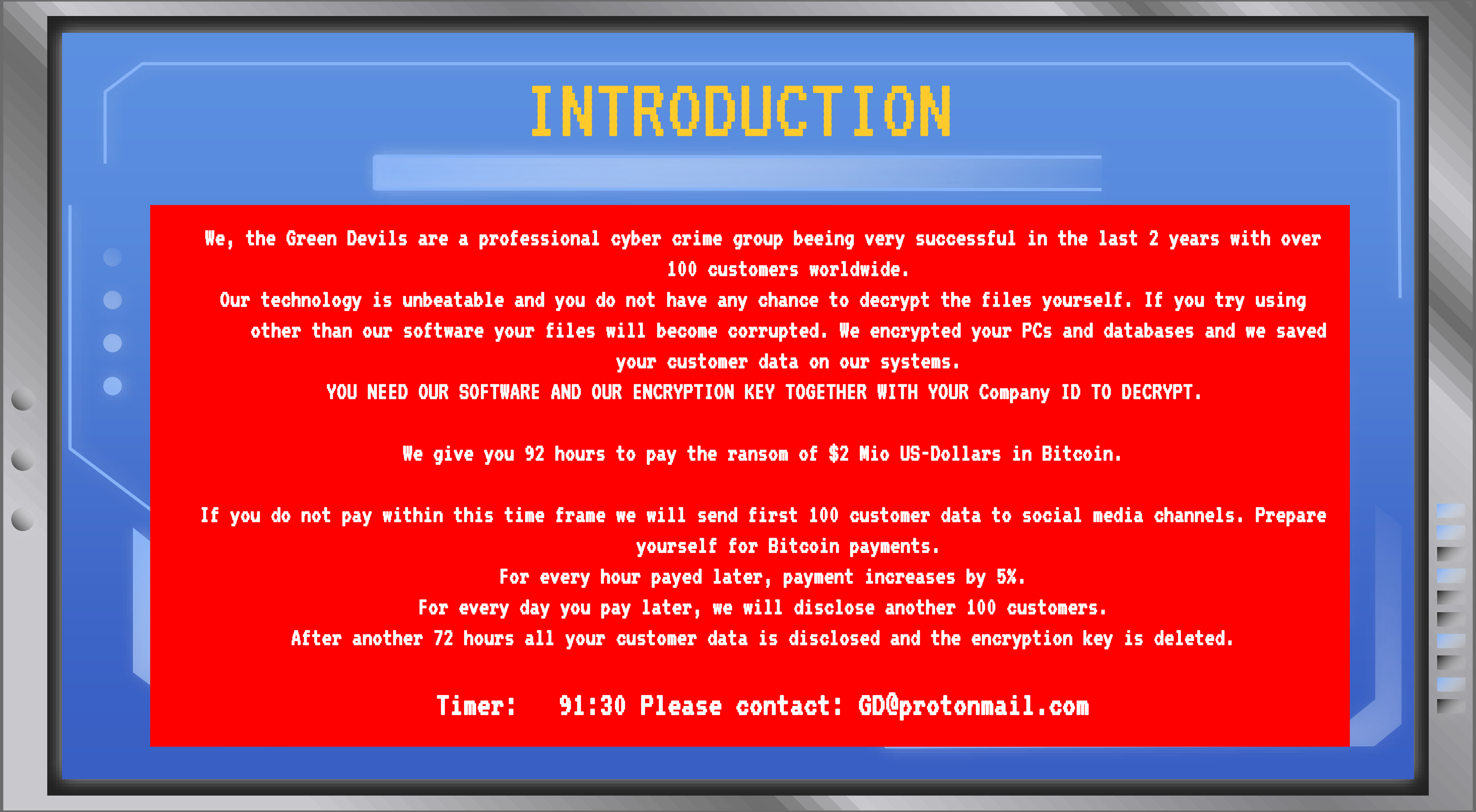
During the day 31.10. (Sunday) the CISO received information about a series of IS Incidents:

INC0012411 - Phishing Mail received
INC0012412 - Phishing Mail received
…
INC0012413 - PC shows Skull, User cannot work
INC0012414 - PC shows Skull, User cannot work
INC0012416 - PC shows Skull, User cannot work
INC0012419 - PC shows Skull, User cannot work
...

IT declares INC0012445 Major Incident because of increasing Incident numbers 12411-12444.

MoD (Manager on Duty) informs CISO by phone call; MiM Service Provider (Major Incident Manager) assigned.

INTRODUCTION



INTRODUCTION

We, the Green Devils are a professional cyber crime group beeing very successful in the last 2 years with over 100 customers worldwide.

Our technology is unbeatable and you do not have any chance to decrypt the files yourself. If you try using other than our software your files will become corrupted. We encrypted your PCs and databases and we saved your customer data on our systems.

YOU NEED OUR SOFTWARE AND OUR ENCRYPTION KEY TOGETHER WITH YOUR Company ID TO DECRYPT.

We give you 92 hours to pay the ransom of $2 Mio US-Dollars in Bitcoin.

If you do not pay within this time frame we will send first 100 customer data to social media channels. Prepare yourself for Bitcoin payments.

For every hour payed later, payment increases by 5%.

For every day you pay later, we will disclose another 100 customers.

After another 72 hours all your customer data is disclosed and the encryption key is deleted.

Timer: 91:30 Please contact: GD@protonmail.com

What do we do first?

01

CISO: Engages Forensic company

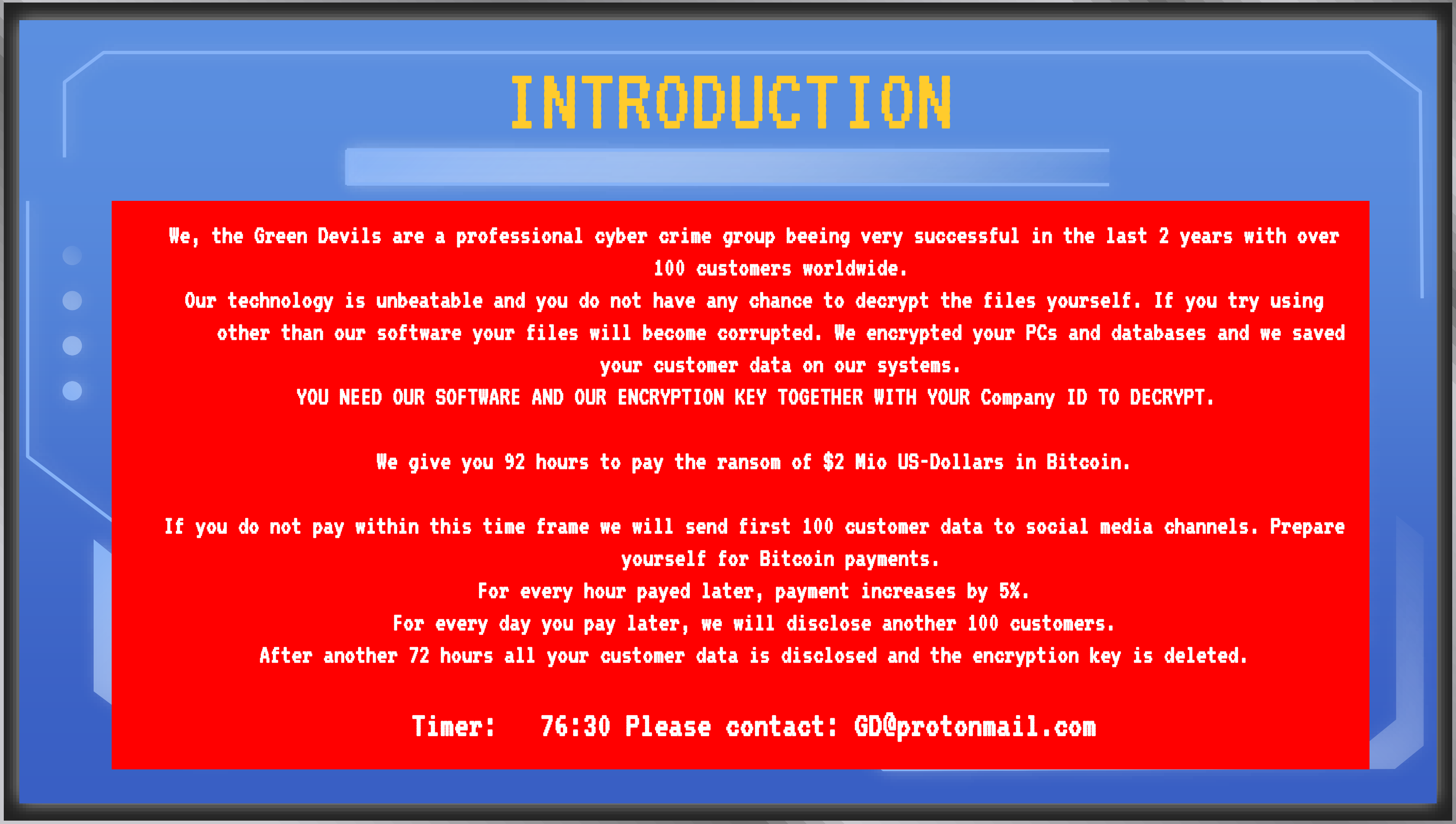
02

CISO: Create MS Teams INC-0012425 and invite participants

03

CISO: Validates IS Emergency, Declares IS Emergency Case by writing email or phoning

Round 01



INTRODUCTION

We, the Green Devils are a professional cyber crime group beeing very successful in the last 2 years with over 100 customers worldwide.

Our technology is unbeatable and you do not have any chance to decrypt the files yourself. If you try using other than our software your files will become corrupted. We encrypted your PCs and databases and we saved your customer data on our systems.

YOU NEED OUR SOFTWARE AND OUR ENCRYPTION KEY TOGETHER WITH YOUR Company ID TO DECRYPT.

We give you 92 hours to pay the ransom of $2 Mio US-Dollars in Bitcoin.

If you do not pay within this time frame we will send first 100 customer data to social media channels. Prepare yourself for Bitcoin payments.

For every hour payed later, payment increases by 5%.

For every day you pay later, we will disclose another 100 customers.

After another 72 hours all your customer data is disclosed and the encryption key is deleted.

Timer: 76:30 Please contact: GD@protonmail.com

PCs infected

Now ~130 PCs show this symbol, up from ~40 31.10. when the IS Emergency Case was declared.

Employees affected so far are from different parts of the organization.

Mail from CISO Pro Network

Hello CISO,

this morning we had an IDS alert of some suspicious network traffic, which appears to beacon to a HTTP server randomly every 50 seconds. We believe that this might be related to a ransomware threat that we recently received and are currently trying to identify the source and destination of this traffic. We suspect that we may not be the only organization targeted by this threat. We recommend you check for possible infections in your network too.

Thanks
CISO Pro

Shops infected

As of 1.11. at 10:00, 25 shops that opened on 1.11. at 9:00 and booted PCs in online mode were infected.

(our other 24 shops are closed on 1.11. because of public holiday)

What needs to be done now?

CISO: Explains situation to SMT, collects action items, creates plan

Containment (further PCs, network, servers) and defense

Business impacts discussed

Initial stakeholder information (Employees, workers council, law enforement authority)

Core Team: Create action plan & communication plan

SMT:
Think about budget and additional help

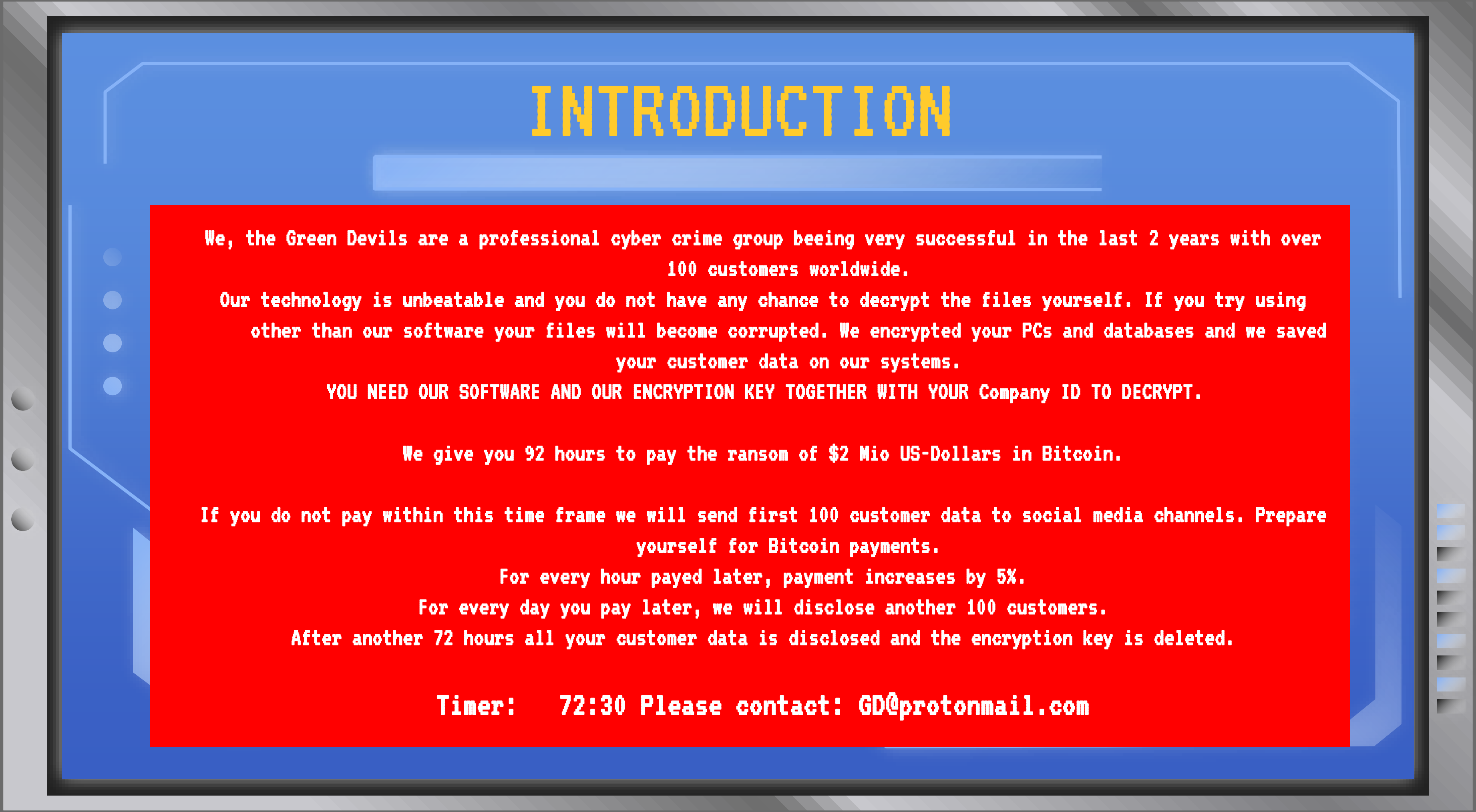
Discuss situation with SMT

Analyze other Incidents in Ticket Tool

Engage Forensic company

Discuss potential Data Protection impact and decide whether/when authorities will be informed

Round 02



INTRODUCTION

We, the Green Devils are a professional cyber crime group beeing very successful in the last 2 years with over 100 customers worldwide.

Our technology is unbeatable and you do not have any chance to decrypt the files yourself. If you try using other than our software your files will become corrupted. We encrypted your PCs and databases and we saved your customer data on our systems.

YOU NEED OUR SOFTWARE AND OUR ENCRYPTION KEY TOGETHER WITH YOUR Company ID TO DECRYPT.

We give you 92 hours to pay the ransom of $2 Mio US-Dollars in Bitcoin.

If you do not pay within this time frame we will send first 100 customer data to social media channels. Prepare yourself for Bitcoin payments.

For every hour payed later, payment increases by 5%.

For every day you pay later, we will disclose another 100 customers.

After another 72 hours all your customer data is disclosed and the encryption key is deleted.

Timer: 72:30 Please contact: GD@protonmail.com

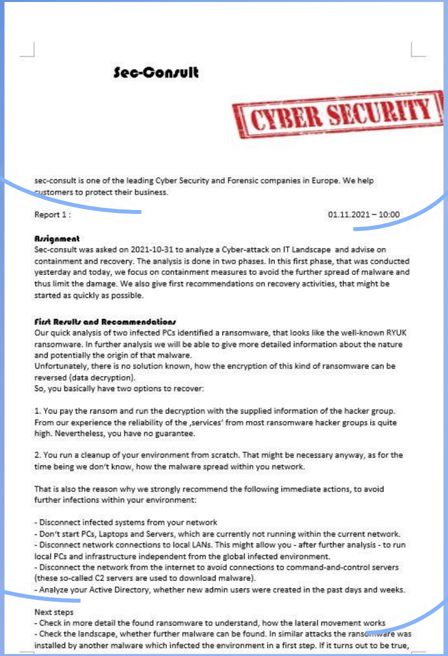
Security Report

Disconnect

- Infected Systems
- Network connections to local LANs
- Network from the internet

Analyze

AD - new admin users created? Compromised?



Sec-Consult

CYBER SECURITY

sec-consult is one of the leading Cyber Security and Forensic companies in Europe. We help customers to protect their business.

Report 1 : 01.11.2021 – 10:00

Assignment

Sec-consult was asked on 2021-10-31 to analyze a Cyber-attack on IT Landscape and advise on containment and recovery. The analysis is done in two phases. In this first phase, that was conducted yesterday and today, we focus on containment measures to avoid the further spread of malware and thus limit the damage. We also give first recommendations on recovery activities, that might be started as quickly as possible.

First Results and Recommendations

Our quick analysis of two infected PCs identified a ransomware, that looks like the well-known RYUK ransomware. In further analysis we will be able to give more detailed information about the nature and potentially the origin of that malware.
Unfortunately, there is no solution known, how the encryption of this kind of ransomware can be reversed (data decryption).
So, you basically have two options to recover:

1. You pay the ransom and run the decryption with the supplied information of the hacker group. From our experience the reliability of the ‚services' from most ransomware hacker groups is quite high. Nevertheless, you have no guarantee.

2. You run a cleanup of your environment from scratch. That might be necessary anyway, as for the time being we don't know, how the malware spread within you network.

That is also the reason why we strongly recommend the following immediate actions, to avoid further infections within your environment:

- Disconnect infected systems from your network
- Don't start PCs, Laptops and Servers, which are currently not running within the current network.
- Disconnect network connections to local LANs. This might allow you - after further analysis - to run local PCs and infrastructure independent from the global infected environment.
- Disconnect the network from the internet to avoid connections to command-and-control servers (these so-called C2 servers are used to download malware).
- Analyze your Active Directory, whether new admin users were created in the past days and weeks.

Next steps
- Check in more detail the found ransomware to understand, how the lateral movement works
- Check the landscape, whether further malware can be found. In similar attacks the ransomware was installed by another malware which infected the environment in a first step. If it turns out to be true,

Check

- Ransomware: Lateral movement
- Landscape: Further malware
- Backups: For infections
- Plan setup of new network segments

More PCs infected

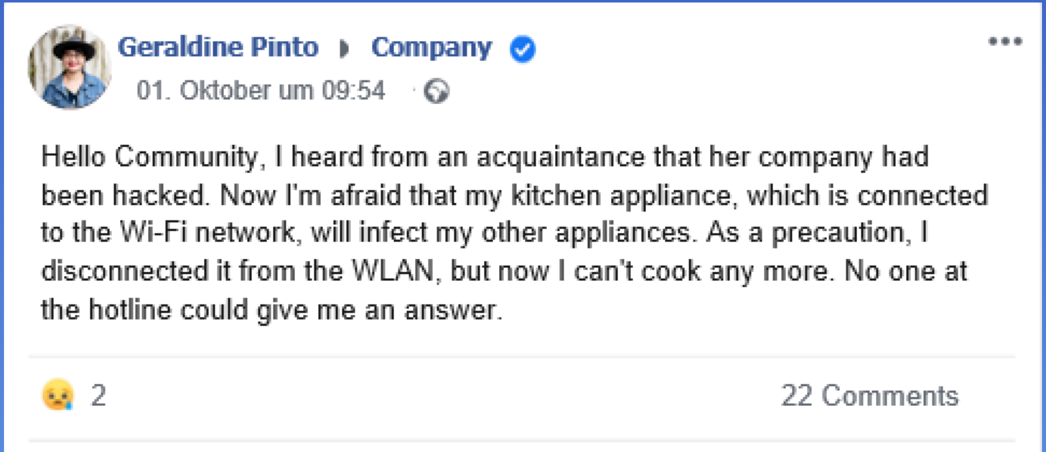
Current overview of IS Incidents show that now more than ~200 PCs show this symbol.

In total around 300 PCs: more than ~200 PCs and more than ~70 in shops.

Applications not reacting

System	Function	Affected users
SAP P01	Sales, Logistics	560 (D, A, F)
CRM	CRM, Sales Orders	500 (D, A, F)
SAP P30	Sales, Logistics, Material Master Data	100 (VIN)
Futura POS Server	Server component of local shop systems	50*2 (D)
HVP	Advisor portal Germany	8000 (D)

Social media post



Geraldine Pinto ▸ Company ✓

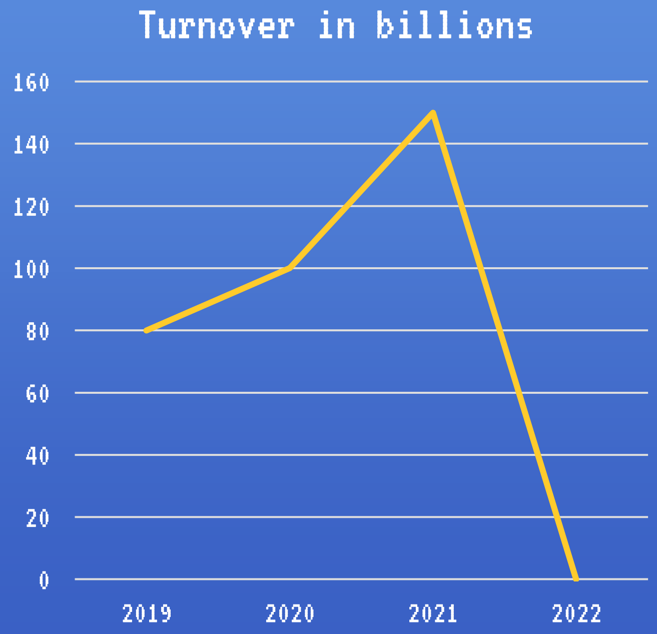
01. Oktober um 09:54 ·

Hello Community, I heard from an acquaintance that her company had been hacked. Now I'm afraid that my kitchen appliance, which is connected to the Wi-Fi network, will infect my other appliances. As a precaution, I disconnected it from the WLAN, but now I can't cook any more. No one at the hotline could give me an answer.

😢 2

22 Comments

Request from sales manager



Dear Ladies and Gentlemen,

Our commercial agents currently have no access to the commercial agent platform and are therefore unable to process orders and payments.

As we cannot estimate when the commercial agent platform will be available again, we would like to ask you to decide which information and recommendations for action we should send to our commercial agents to place orders and pay out commissions.

Yours sincerely
Gordon Gekko, Germany Sales Management

Call from News Paper to Head of Press Office

Hello press office

Is it true that you have been hacked?
According to our sources, various employees and sales staff have no longer have IT access.
Can you confirm this?
What does this mean for owners of a kitchen appliance or a robot vacuum cleaner?
Have these devices also been hacked?
If so, what are the consequences, how can your customers behave?
How high do you estimate the total damage?
What are you doing now?
How long will it take you to get the problem under control?

The press office has asked the News Paper for **an hour** to think about the questions
and is now asking for guidance on the answers.

What needs to be done now?

Advise shops to take off POS from network and work in offline mode

Alternative work scenarios for shops and sales representative ?

Isolate all infected systems; separate network segments to the maximum possible extend; specifically, the network of production sites should be separated

Requests proposals for emergency operations from IT Service and from Business (e.g. Offline form for Sales Orders)

Request analysis of admin users created

Request to analyze activities of new Domain-Admins

Ask Group IT/Service Provider to check availability of un-encrypted backups / Ask them to analyze recovery procedure and timing

Request IT to prepare for clean network segments for potential recovery activities

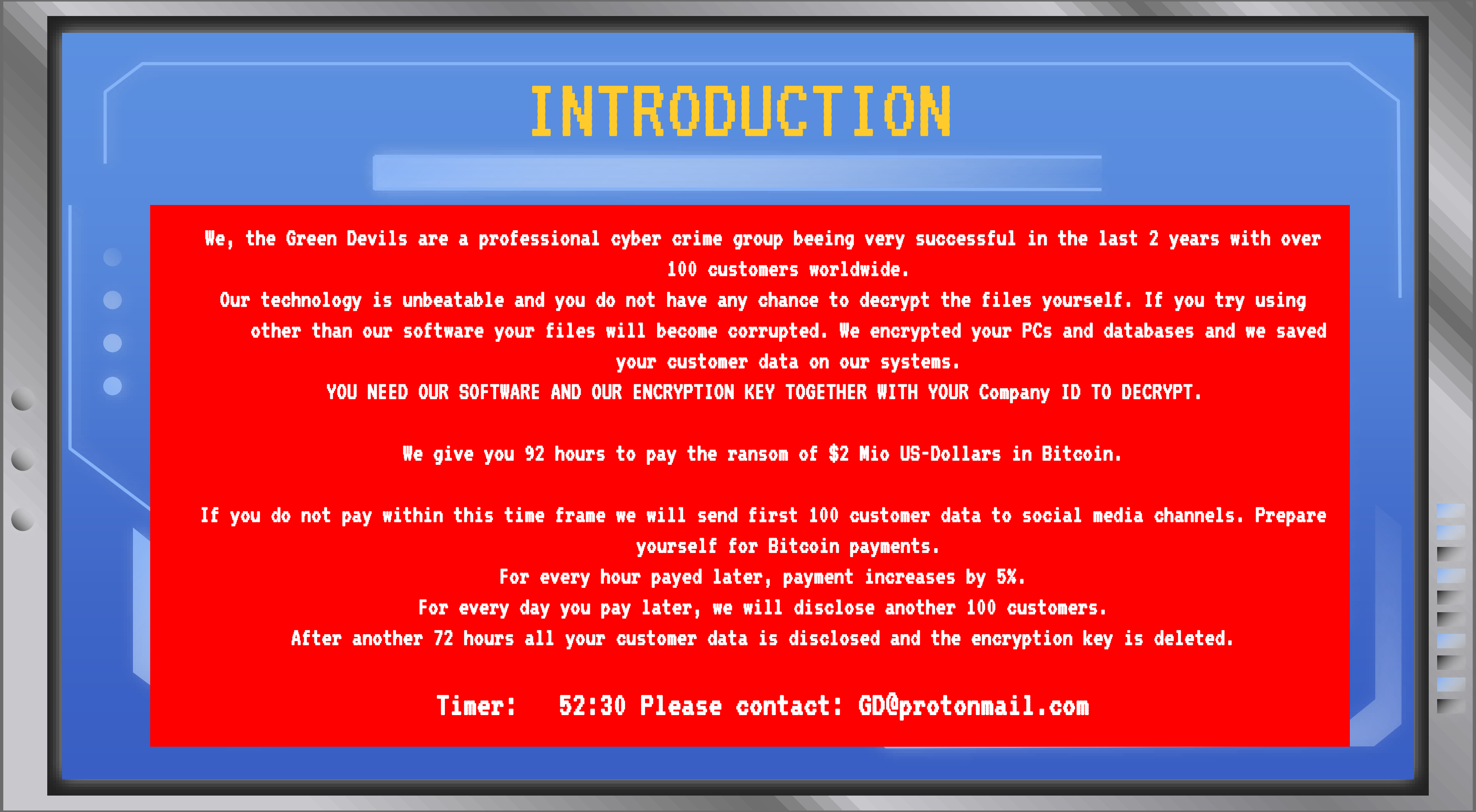
Evaluate contact with Hackers (what do they want, what do they have in their hands)

Evaluate necessary steps for potential bitcoin payments

Communication strategy and watch on social media / how to reach employees

Discuss options to reach employees in order to prevent further spread (do not connect PC to company network)

Round 03



INTRODUCTION

We, the Green Devils are a professional cyber crime group beeing very successful in the last 2 years with over 100 customers worldwide.

Our technology is unbeatable and you do not have any chance to decrypt the files yourself. If you try using other than our software your files will become corrupted. We encrypted your PCs and databases and we saved your customer data on our systems.

YOU NEED OUR SOFTWARE AND OUR ENCRYPTION KEY TOGETHER WITH YOUR Company ID TO DECRYPT.

We give you 92 hours to pay the ransom of $2 Mio US-Dollars in Bitcoin.

If you do not pay within this time frame we will send first 100 customer data to social media channels. Prepare yourself for Bitcoin payments.

For every hour payed later, payment increases by 5%.

For every day you pay later, we will disclose another 100 customers.

After another 72 hours all your customer data is disclosed and the encryption key is deleted.

Timer: 52:30 Please contact: GD@protonmail.com

Feedback from IT Service on affected systems

Since Sunday 31.10, when ransomware was detected, we analyzed our landscape for potential infections which will last around another 2-3 hours as we have hundreds of servers.

So far we can say that no more than the systems in the following two injects are affected.

- P01 was shut down
- Employees were sent home
- All other systems also shut down

And more PCs infected

Current overview of IS Incidents show that now more than ~500 PCs show this symbol.

Additionally, we see several home office PCs infected ~ 80.

Repair Center PCs were infected as well: 20 PCs

In total around 700 PCs (including shops infected). Macs and company smartphones are not affected.

Backup information of applications infected

System	Function	Data backup media
SAP P01	Sales, Logistics	Daily on Disk DellEMC
CRM	CRM, Sales Orders	Daily on Disk DellEMC
SAP P30	Sales, Logistics, Material Master Data	Daily on Disk DellEMC
Futura POS Server	Server component of local shop systems	Daily on Disk DellEMC
HVP	Advisor portal Germany	Daily by Service Provider

Backup/Recovery Details: Clients

Before! Make sure network segment for installation is not infected and separated from company or wait for clean new network.

New installation of PCs and Laptops: **8 hours**

We have 4 employees in Field Service and each can do a max of 10 in parallel (need LAN not WLAN).

Employees are asked to bring their PC/Laptop to the central Field Service.

New installation of shops: **5 hours**

We have 3 IT field service employees. One field service employee can do 2-3 PCs in these 5 hours. They have to travel to a shop. We can allocate additional dispatched service employees but with some upfront time of 1 day at least.

Backup/Recovery Details: Server

Answer from Group IT:

Backups of SAP systems are **unencrypted** and can be used for recovery! Retention period 28 days.

Recovery:

Separate all SAP servers from network first - SAP DB Server (Database Oracle) recovery (application servers are not affected)

We estimate a minimum of 2 days per system.

We need 2 SAP Basis Experts and one key user per module for testing.

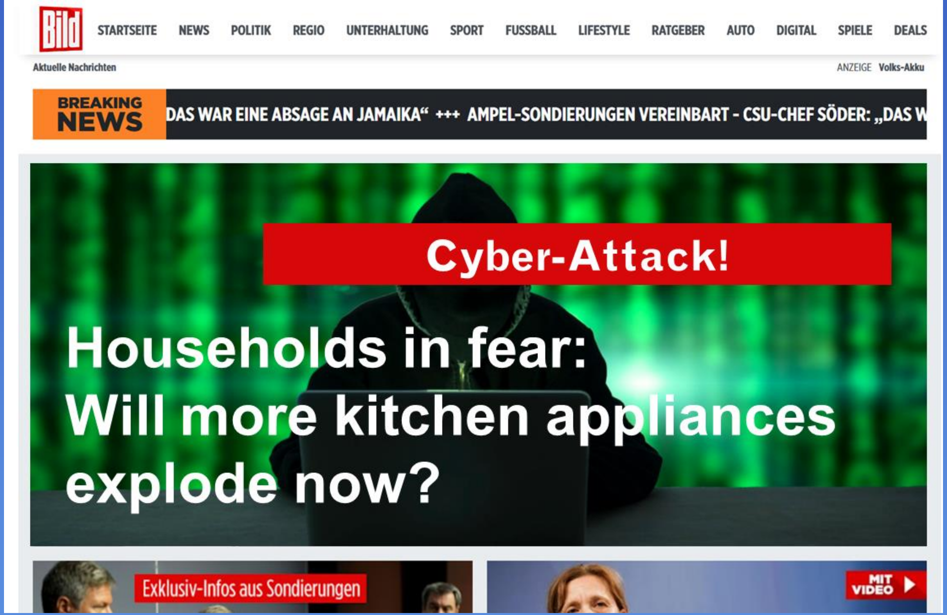
Restore from Data Backup - Oracle rman backup

Test system functionality by SAP Basis, Test by key users

Data Gap to be analyzed: Lost records

In total we estimate **3 days for SAP systems** to be up and running and another week at least to analyze and close data gaps caused by not running interfaces. We need key users for all systems for support .

The press: Bildzeitung



BREAKING NEWS DAS WAR EINE ABSAGE AN JAMAIKA“ +++ AMPEL-SONDIERUNGEN VEREINBART - CSU-CHEF SÖDER: „DAS W

Cyber-Attack!

Households in fear:
Will more kitchen appliances explode now?

Exklusiv-Infos aus Sondierungen

Law Enforcement

CISO involved LKA & ZAC actively

We would like to inform you about a similar attack at another German company which is also infected.
We know from experience that this particular hackergroup most likely did not extract large amounts of data.
We would like to offer help in forensic analysis.
We can ensure a constructive interaction and confidentiality.

LKA = Landeskriminalamt → State Office of Criminal Investigation
ZAC = ZAC Zentrale Ansprechstellen Cybercrime → Central Cybercrime Contact Points

Call from Supervisory Board

Dear members of the Executive Board,

Thank you for the timely information about the hacking attack that took place. We would like to ask you for further information:

What damage was caused?
What countermeasures are being taken?
What can the Advisory Board contribute to solving the problem?

Please keep us informed about further events.

Yours sincerely

Supervisory Board

What needs to be done now?

Business Impact Analysis (financial, reputation) vs. Bitcoin payments

backup estimation overall clean network setup (3 days), then (servers~5 days) and (PCs~20 days)-> in total 23 days

Production discussion (when no sales orders are created)

Request Hacker Group to present leaked data example (email)

How to reach employees (at home without PCs, with encrypted PCs and in office environment)

Conclusion after 9 rounds

Progress after 4 weeks

It took 4 weeks to recover

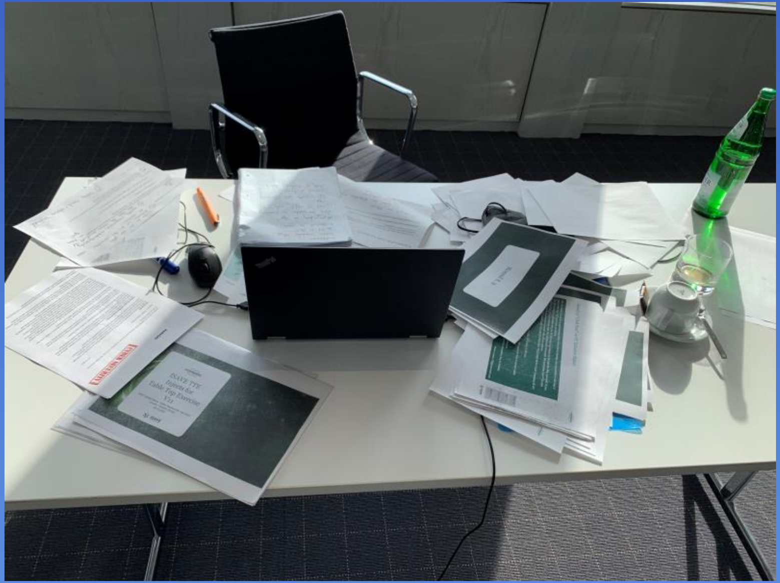
Additional external IT Service technicians were hired for PC recovery of remote locations

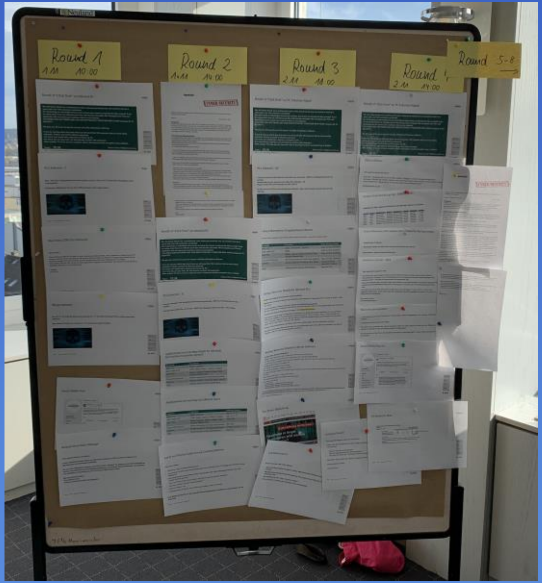
There are still data gaps to be analyzed because interfaces were not running during the shutdowns (manual work)

Social Media now quieter

Servers were up and running after 9 days, but Application Recovery lasted longer due to tests, integrity checks and manual data corrections

4-hour exercise



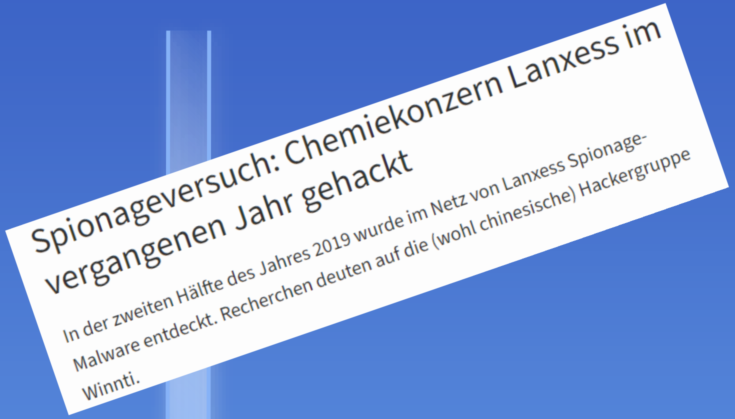


Participants: COO, CFO, CIO, CISO, Head of Communications / Data Protection / IT Security / Finance Switzerland, Member of IS Group, + external consultants

RODNI

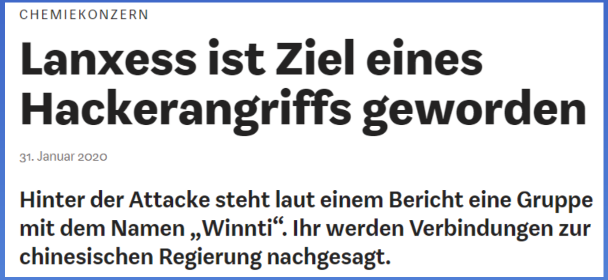
Return on "damages not incurred"

2019: LANXESS



Spionageversuch: Chemiekonzern Lanxess im vergangenen Jahr gehackt

In der zweiten Hälfte des Jahres 2019 wurde im Netz von Lanxess Spionage-Malware entdeckt. Recherchen deuten auf die (wohl chinesische) Hackergruppe Winnti.

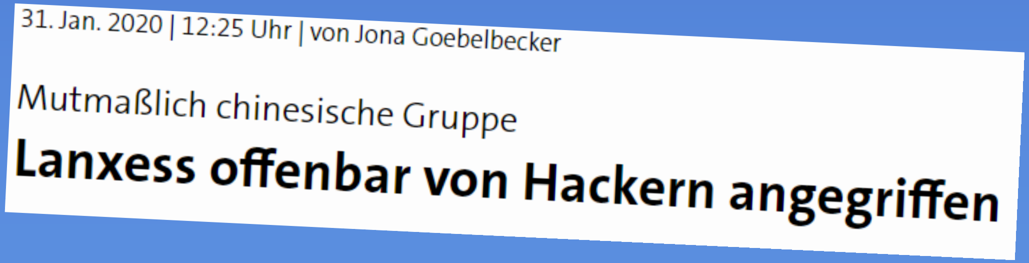


CHEMIEKONZERN

Lanxess ist Ziel eines Hackerangriffs geworden

31. Januar 2020

Hinter der Attacke steht laut einem Bericht eine Gruppe mit dem Namen „Winnti“. Ihr werden Verbindungen zur chinesischen Regierung nachgesagt.

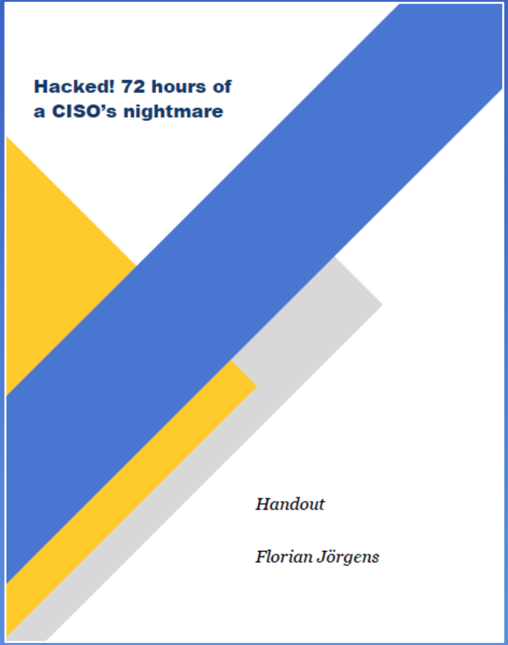


31. Jan. 2020 | 12:25 Uhr | von Jona Goebelbecker

Mutmaßlich chinesische Gruppe

Lanxess offenbar von Hackern angegriffen

Handout



Hacked! 72 hours of a CISO’s nightmare

Handout

Florian Jörgens

- **Communication**
  - internal
  - External
  - Templates

- **Service-Partner**
  - Overview global
  - Overview local

- **Technical Topics**
  - SMS-Gateway
  - Network Segmentation
  - Backup & Recovery
  - Crisis Documentation
  - Processes
  - Emergency Shutdown
  - Recovery Process

Florian Jörgens

Questions?

linkedin.com/in/florian-jörgens/