



# Share experience. Build resilience

Welcome to SECCON NL 2022

digital trust  
center.



HSD  
securitydelta.nl

CYBERVEILIG  
NEDERLAND



Nationaal Cyber Security Centrum  
Ministerie van Veiligheid en Justitie

telindus  
a Proximus company

avit

CISCO  
SECURE



# How to break a Datacenter?

Fred Streefland  
CEO, Secior  
22 Sep 2022



*“Without datacenters, there  
would be no internet!”*



# Agenda

- 1 Introduction
- 2 What is a datacenter?
- 3 IT - OT - IoT Convergence
- 4 How to break a datacenter?
- 5 Q & A



# Introduction



# INTRODUCTION



## Fred Streefland, EMSD, bc.

- ❑ Since 1992 working in the intelligence & security domain
- ❑ Netherlands Air Force (RNLAf), IBM, Accenture, ENCS, Exact Software, LeaseWeb, Palo Alto Networks, Hikvision
- ❑ CEO, Secior

# secior.

## Secior

- ❑ 100% Dutch company, with a focus on **3D Cybersecurity of Datacenters**
- ❑ Unique combination of:
  - 20+ years on datacenter development, construction and operations
  - 20+ years IT/OT/IoT cybersecurity
  - 20+ years on IT audits & red-teaming



# INTRODUCTION



## OVH data center fire likely caused by faulty UPS power supply

By [Ax Sharma](#)

📅 March 12, 2021


🕒 02:45 AM






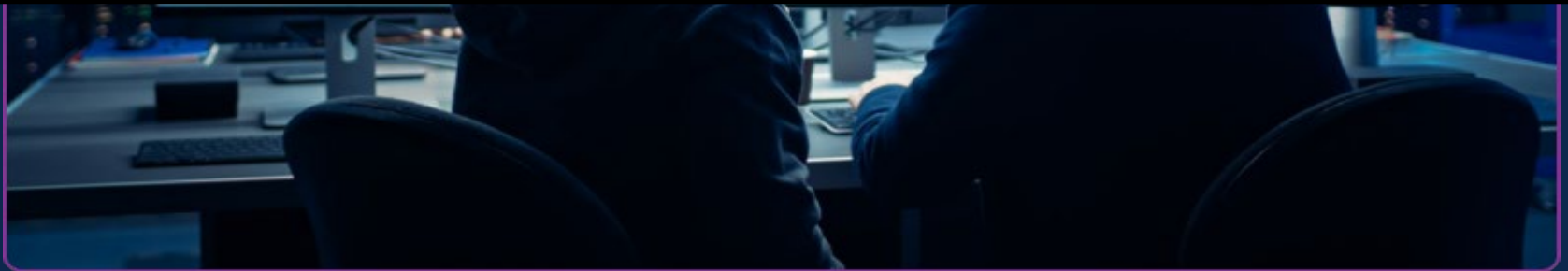
## Over 20,000 data center management systems exposed to hackers

By **Bill Toulas**

 January 29, 2022

 11:08 AM

 1







# INTRODUCTION

RESEARCH — 12 Apr, 2022

## How the war in Ukraine could impact data centers



Author **Kelly Morgan**  
Theme **Corporates, Technology, Media & Telecom**  
Segment **Corporations**  
Tags **Global**



World ▾ Business ▾ Legal ▾ Markets ▾ Breakingviews Technology ▾ Investigations

April 20, 2022  
8:40 PM GMT+2  
Last Updated 5 months ago

Europe

## West warns of Russian cyberattacks on critical infrastructure

By James Pearson

2 minute read



nozominetworks.com

8

TABLE OF CONTENTS INTRODUCTION **THE THREAT LANDSCAPE** THE IOT BOTNET LANDSCAPE THE VULNERABILITY LANDSCAPE RECOMMENDATIONS FORECAST REFERENCES

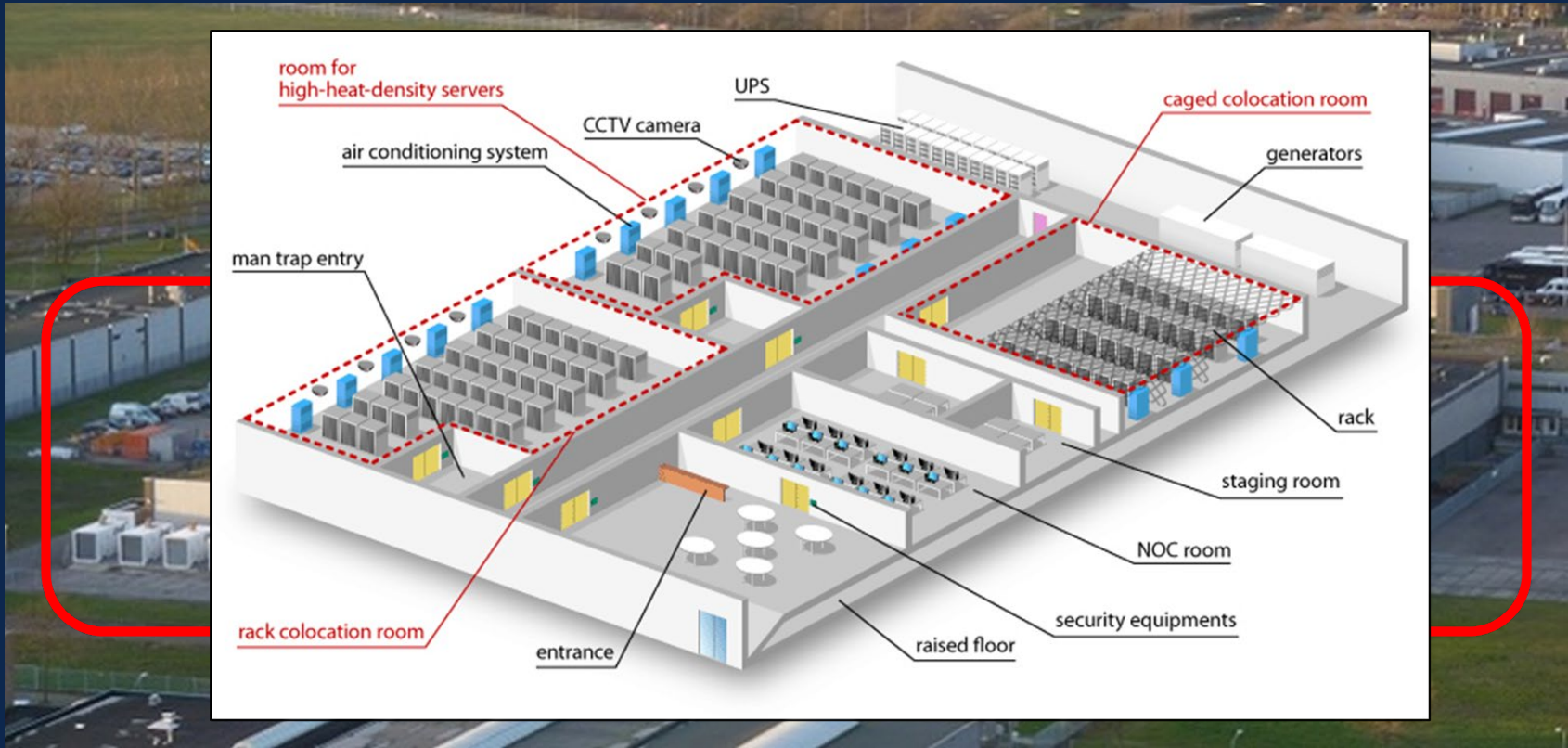


## 2.2 Russia/Ukraine War Spikes Cyber Activity



# What is a datacenter?

# WHAT IS A DATACENTER?



# WHAT IS A DATACENTER?



Cooling & Ventilation systems (OT)



Power & Distribution systems (OT)



Smoke/Fire Detection systems (OT)



Monitoring systems (IoT)



Rack locks (IoT)



DCIM (IT)



# WHAT IS A DATACENTER?

## Power & Distribution systems (OT)

- Transformers
- Uninterruptible Power Sources (UPS)
- Rack Power Distribution Units (PDUs)
- .....

## Environmental control systems (OT)

- Chillers
- Computer Room Air Conditioners (CRACs)
- Heating, Ventilation & Air Conditioning (HVAC) systems
- .....

## Security/Detection/Measurement systems (IoT)

- CCTV devices
- Fire dampers/VESDA
- Temperature/Air/Pressure valves/sensors
- .....

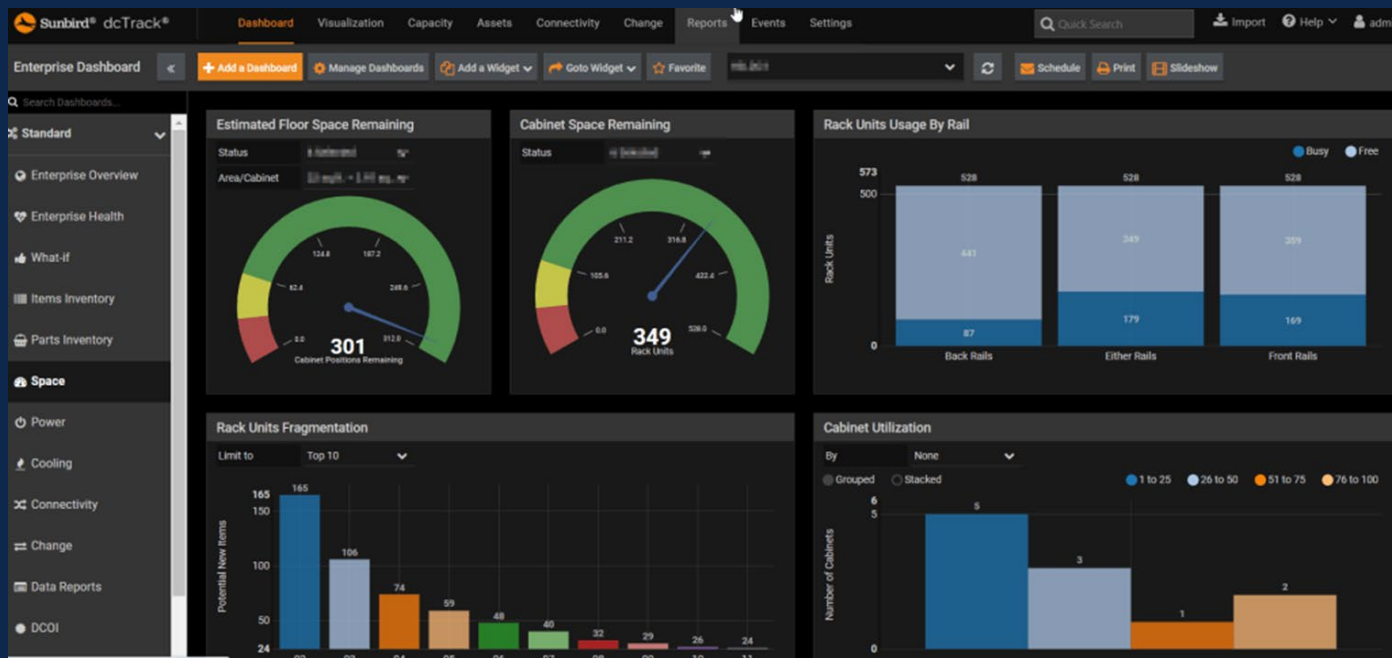
## DCIM (OT)





# WHAT IS A DATACENTER?

## Datacenter Infrastructure Management System (DCIM) Dashboard

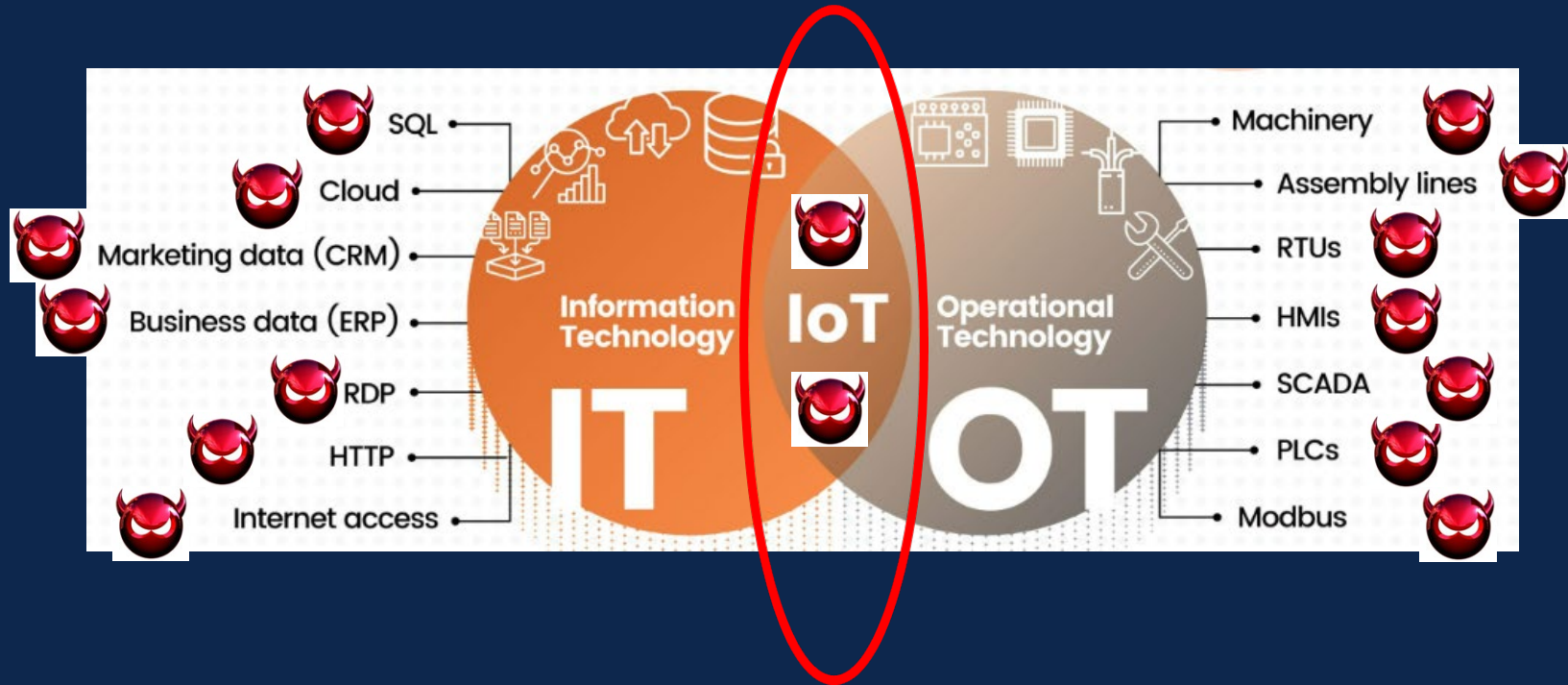


Share experience. Build resilience.

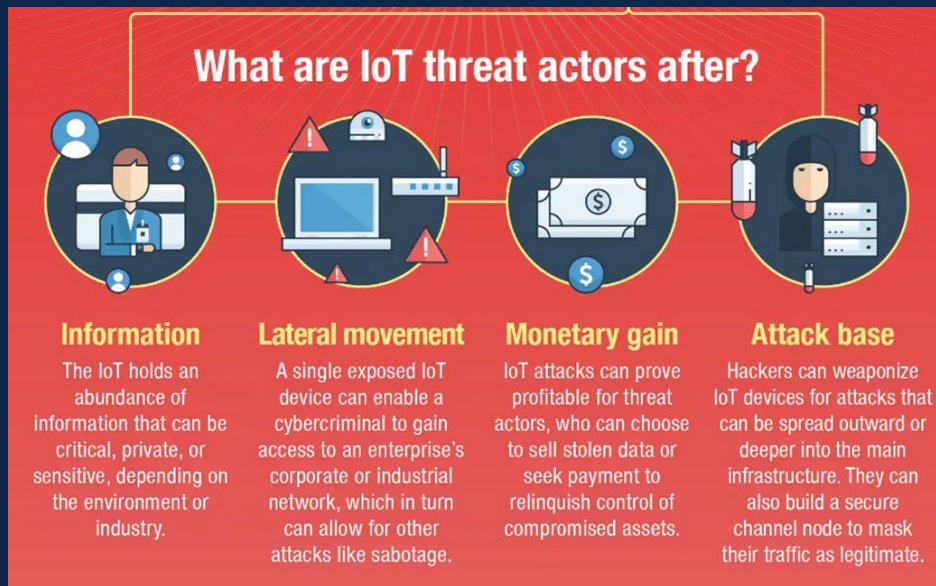


# IT- OT – IoT Convergence

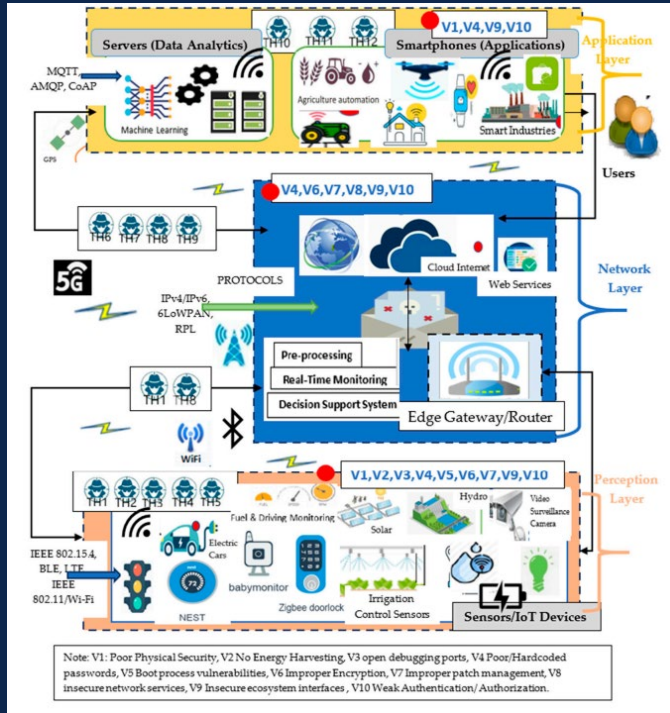
# IT-OT-IoT CONVERGENCE







## IoT threat architecture



## OWASP Top 10 Attack Surface areas

- 1) Weak, guessable or hardcoded passwords;
- 2) Insecure network services;
- 3) Insecure ecosystem interfaces;
- 4) Lack of secure update mechanism;
- 5) Use of insecure/outdated software components;
- 6) Insufficient privacy protection;
- 7) Insecure data transfer and storage;
- 8) Lack of device management;
- 9) Insecure default settings;
- 10) Lack of physical hardening

Source: <https://pdfs.semanticscholar.org/3d40/93e114af81d94fa87406407207c295c4998b.pdf>



# How to break a datacenter?

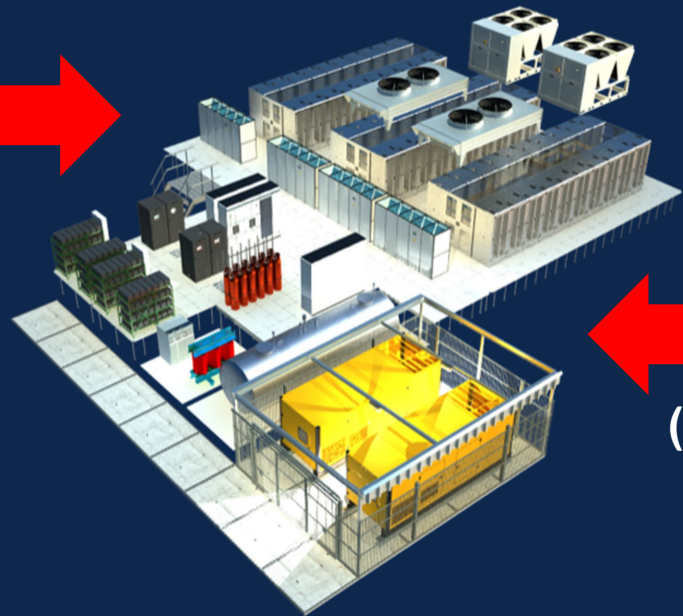
# HOW TO BREAK A DATACENTER?



Attack 1



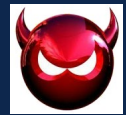
(UPS)



Attack 2



(CRACs + DCIM)



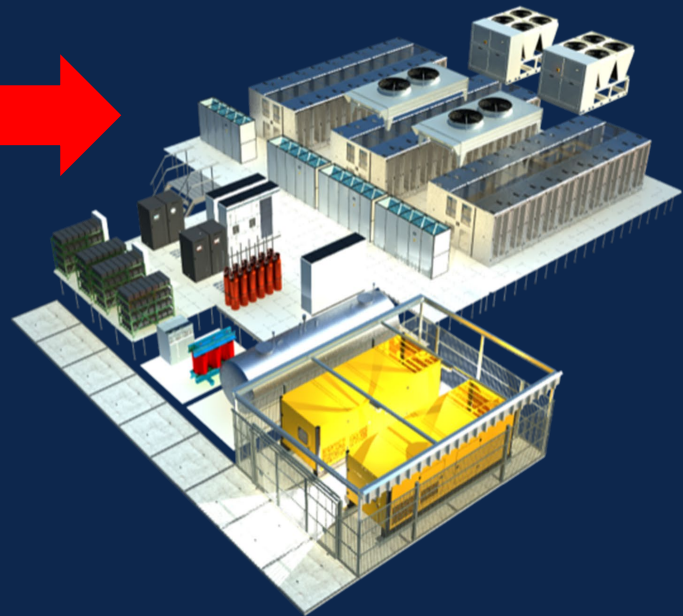
# HOW TO BREAK A DATACENTER?



Attack 1



(UPS)



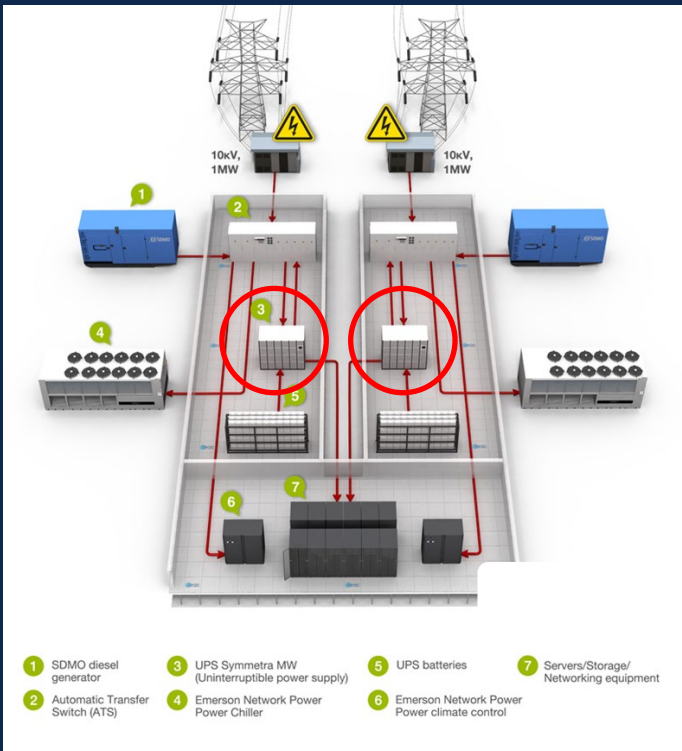
# HOW TO BREAK A DATACENTER?



Attack 1



(UPS)

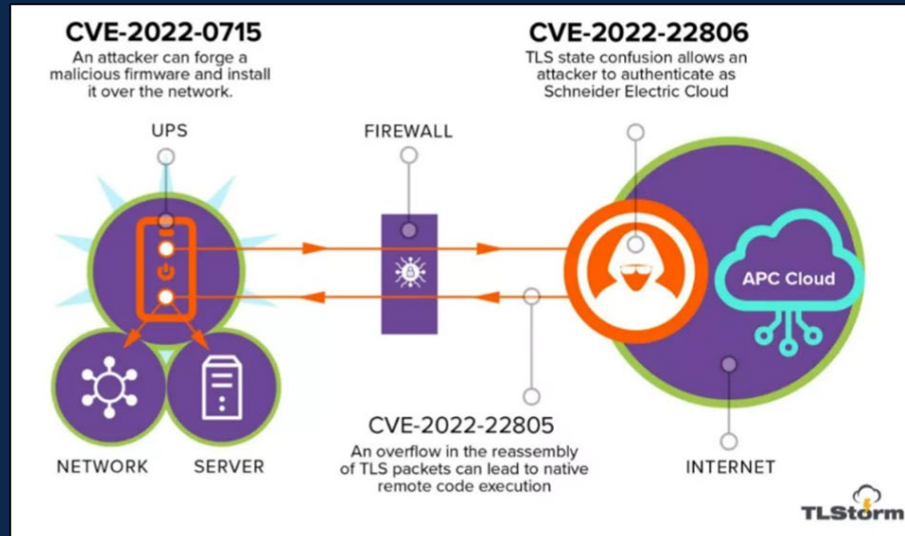


# HOW TO BREAK A DATACENTER?

## Researchers discover critical vulnerabilities in APC Smart-UPS devices

The vulnerabilities can result in remote manipulation and potential damage to other controlled assets

By [Jimmy Pezzone](#) March 13, 2022 at 8:47 AM | [10 comments](#)





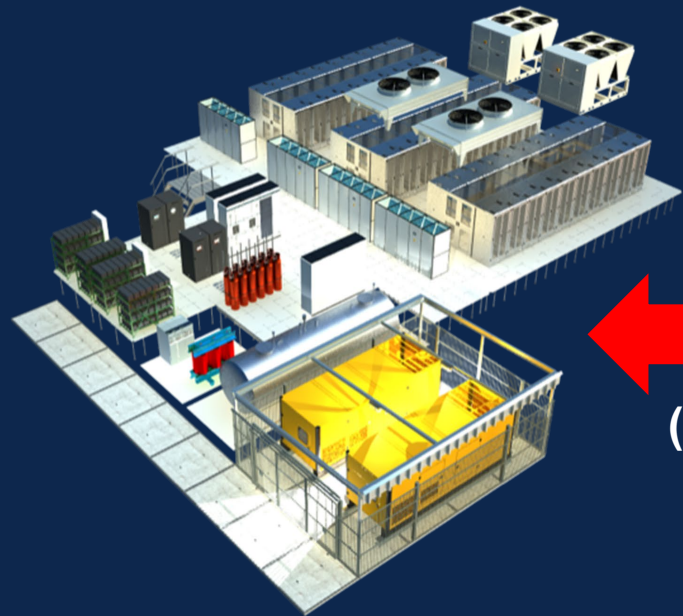
# HOW TO BREAK A DATACENTER?

The UPS is now bricked and will not turn on even after the smoke clears out.



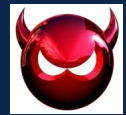


# HOW TO BREAK A DATACENTER?



**Attack 2**

**(CRACs + DCIM)**



# HOW TO BREAK A DATACENTER?



# HOW TO BREAK A DATACENTER?

The screenshot displays the Shodan search engine interface. At the top, there is a navigation bar with the Shodan logo, links for 'Explore' and 'Pricing', a search bar containing the query 'stulz', and a 'Login' button. Below the navigation bar, the main content area is divided into several sections:

- TOTAL RESULTS:** Shows a count of 19 results.
- TOP COUNTRIES:** A world map with a list of countries and their corresponding result counts:

Country	Count
Viet Nam	5
Germany	2
Spain	2
Greece	2
Bangladesh	1

A 'More...' link is provided below the list.
- TOP PORTS:** Shows a count of 80 results for port 80.
- Search Results:** The main section displays two search results. The first result is for IP address 94.220.6.212, with details including:
  - Hostnames: dslb-094-220-006-212.094.2, 20.pools.vodafone-ip.de, ARCOR AG
  - Location: Germany, Hamburg
  - Service: Snmp
  - Version: 1
  - Uptime: 151502668
  - Description: Stulz GmbH Klimatechnik W18 8000
  - Location: aircondition
  - Order: The MIB Module from SNMPv2 entities
  - Contact: local admin, aber bitte einer, der lesen kann und es auch macht. Es geht noch weiter. Object...The second result is for IP address 195.251.140.27, with details including:
  - Hostnames: admin-aircond, University of the Aegean
  - Location: Greece, Mytilene
  - Service: HTTP/1.0 200 OK
  - Server: Stulz GmbH Klimatechnik embedded Web Server v2.0
  - Content-Type: text/html; charset=utf-8
  - Expires: 0
  - Cache-Control: max-age=0
  - Connection: keep-alive

# HOW TO BREAK A DATACENTER?

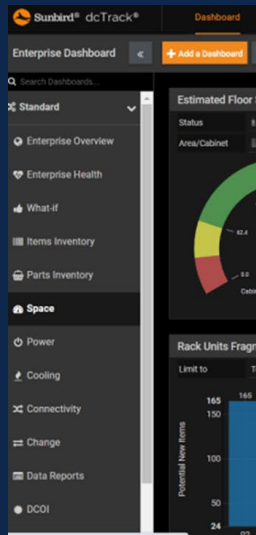
## Over 20,000 data center management systems exposed to hackers

By [Bill Toulas](#)

January 29, 2022

11:08 AM

1



### Temperature & Humidity: Integrated Temperature Sensor

Name:

Location:

Alarm Status: ✔ Normal

Temperature: 21.0° C

#### Temperature Thresholds

Maximum:  ° C [0 to 60]

High:  ° C [0 to 60]

Low:  ° C [0 to 60]

Minimum:  ° C [0 to 60]

Hysteresis:  ° C [0 to 10]

Apply

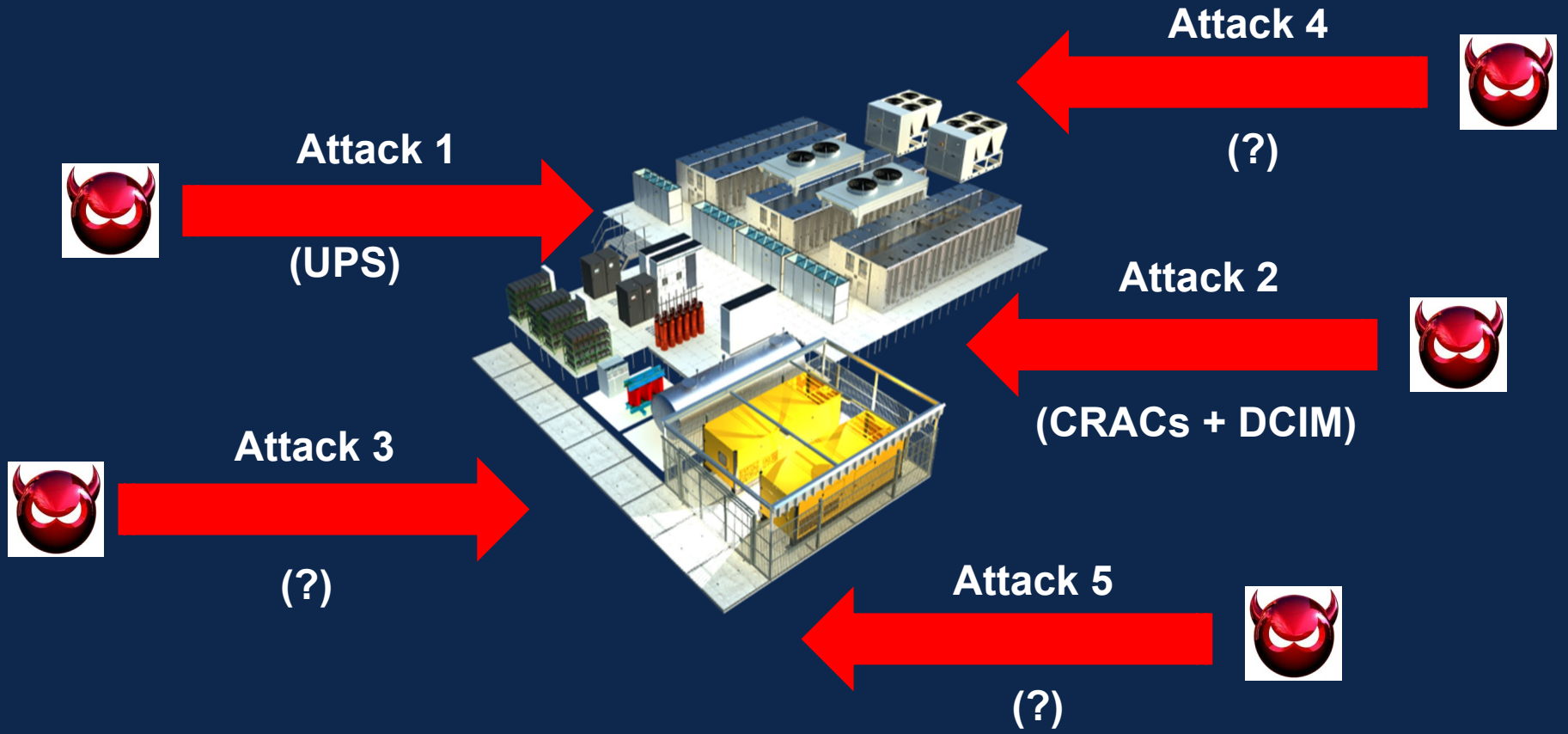
Cancel

Accessing temperature threshold settings

Source: *Cyble*



# HOW TO BREAK A DATACENTER?





*“The most effective way to sabotage multiple servers or an entire datacenter is a cyberattack on the technical infrastructure.”*

*It is easier to shut down a datacenter by disabling the cooling system than by attacking each of the servers”*



# Ask me anything

Share experience. Build resilience.

# SECCON-NL 2022

Share experience. Build resilience

Time

09:00 – 10:00

Opening Keynote Sadie Creese (Professor Cybersecurity @ Oxford University)

Main stage (Zliversmederij 300 seats)

Breakout room 1 (Penningzaal 80 seats)

Breakout room 2 (Depot 80 seats)

Breakout room 3 (Stempelkamer 60 seats)

Breakout room 4 (Schatkamer 30 seats)

10:00 – 10:15

Break – switch to main stream

Threat Intell

Threat Intel

Post Quantum Security

Threat Intel

AI

10:15 – 10:45

Threat Intel update from Talos – Martin Lee (Talos Threat intelligence organization)

No More Leaks Project – Felix Nijpels (Dutch Police)

The Impact of Quantum on security – a general outlook – Sam Samuel (Cisco)

Threat management at the Dutch Railway – Dimitri van Zantvliet Rozemeijer (Chief Cyber Dutch Railway)

Get ready for the AI attack bot – Richard de Vries (Tata Steel)

10:45 – 11:00

Break – switch to main stream

Detection and Response

SOAR

Post Quantum Security

Detection and Response

Detection and Response / AI

11:00 – 11:30

Day in life at the Dutch Tax Office SOC – Karl Lovink (Belastingdienst)

Stay Ahead of the Game: Automate your Threat Hunting Workflows – Christopher van der Made (Cisco)

Quantum hurdles: an optimistic view of post-quantum security – Sander Dorigo (Fox Crypto)

What Cyber can learn from Biology? – Koen Hokke (KPN)

Unsupervised Anomaly-Based Network Intrusion Detection Using Auto Encoders for Practical Use – Julik Keijer (Northwave)

11:30 – 11:45

Break – switch to main stream

Detection and Response

Detection and Response

DevSecOps/ Detection and Response

DevSecOps

11:45 – 12:15

Compliancy vs security. Pentesting is dead – Edwin van Andel (ZeroCopter)

Incident Response without compromise. How to prepare for the worst day of your career with dice! – Wouter Hindriks (Avit)

Threat Modelling: it's not just for developers – Timothy Wadhwa-Brown (Cisco)

Changed responsibilities in modern software development environments – Martin Knobloch (Microfocus)

How to break a data center? Fred Streefland (Secior)

12:15 – 13:00

LUNCH

13:00 – 13:45

Panel Discussion with Liesbeth Holterman (host CVNL) Koen Sandbrink (NCSC), Jochem Smit (Northwave), Oscar Koeroo (Min Ezk), Jan Heijdra (Cisco)

13:45 – 14:00

Break – switch to main stream

Threat intel / Detection and Response

Threat Intel

Detection and Response

DevSecOps

14:00 – 14:30

CERT in Ukraine experience sharing by Andrii Bezverkhyi (SOCPrime)

This is why you will fail: Most successful attack scenarios and their defenses – Tijme Gommers (Northwave)

Risk-based Auth & ZTA – Frank Michaud (Cisco)

Creating clarity and unity in security standards and guidelines – OpenCRE.org – Rob van der Veer (Software Improvement Group)

(Placeholder) WICCA Breakout (with Wendy joining)

14:30 – 14:45

Break – switch to main stream

Detection and Response

Detection and Response

Detection and Response

Threat Intel

Detection and Response / AI

14:45 – 15:15

Advanced Attacker Automation: Botnet capabilities and techniques used to evade your defences – David Warburton (F5)

Security Maturity: from XDR to SIEM – Gilles van Heijst (Orange Cyber Defense)

Improving Business Security by implementing Security.txt – Julius Offers (Digital Trust Center)

Tackling the challenge of translating threat intelligence into actual action – Raymond Bierens (Connect2Trust)

Fostering emerging technologies in cybersecurity, to reinforce our strategic autonomy. – Christian van der Woude (Dcypher)

15:15 – 16:00

Closing Keynote – Wendy Nather