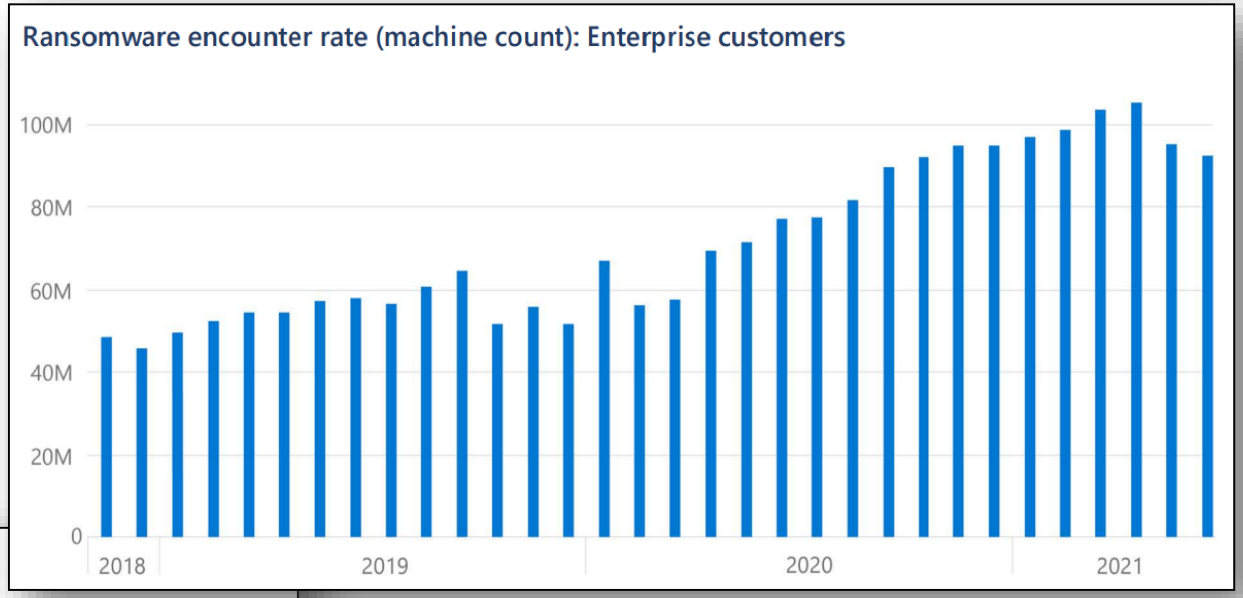
CENTRE FOR CYBER SECURITY

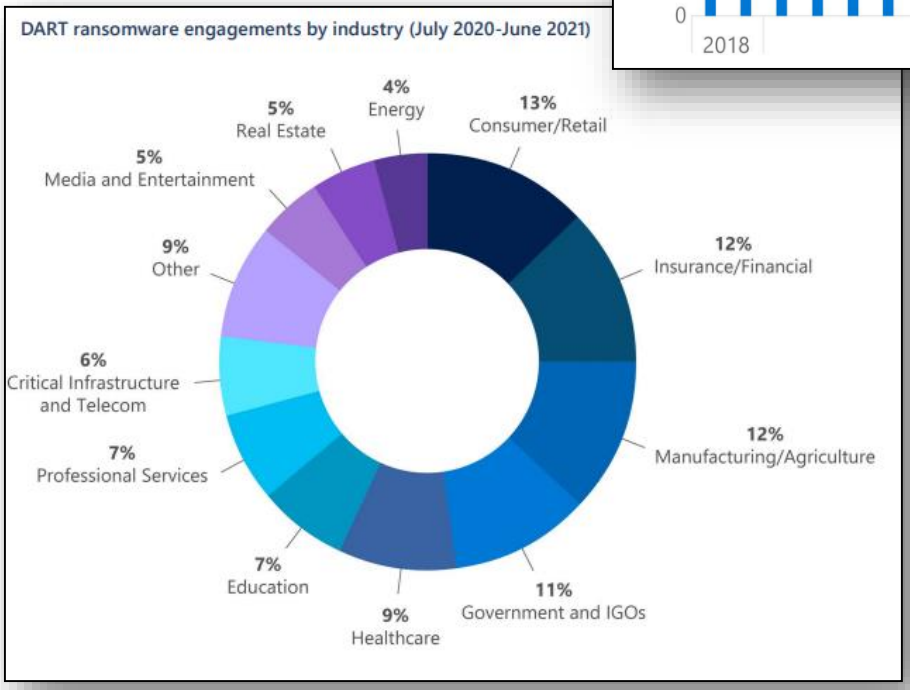
Ransomware

Threat from ransomware on the telecoms sector

CFCS threat assessment department
Jens Oggesen

The threat is **VERY HIGH**





Any organization is a potential target

Source: Microsoft Digital Defense Report 20021

CENTRE FOR CYBER SECURITY

How ransomware works

- Breaching the perimeter
- Automated attacks
- Human-operated attacks (RaaS)
- Data theft and leak

Conti leak-site

Herr
Wolfgang Riedl
Kastanienweg 8
34311 Naumburg

Anschlussanschrift:
Kastanienweg 8, 34311 Naumburg

26. November 2019

Zugangsdaten für das Kundenportal

Guten Tag Herr Riedl,

anbei erhalten Sie Ihre Zugangsdaten für das Kundenportal auf unserer Homepage (www.netcom-kassel.de).

Ihre Zugangsdaten für die genannte Anwendung lauten wie folgt:
Benutzerkennung: 615288
Kennwort: [redacted]

Bitte beachten Sie, dass das Kennwort aus datenschutzrechtlichen Gründen geändert werden musste.

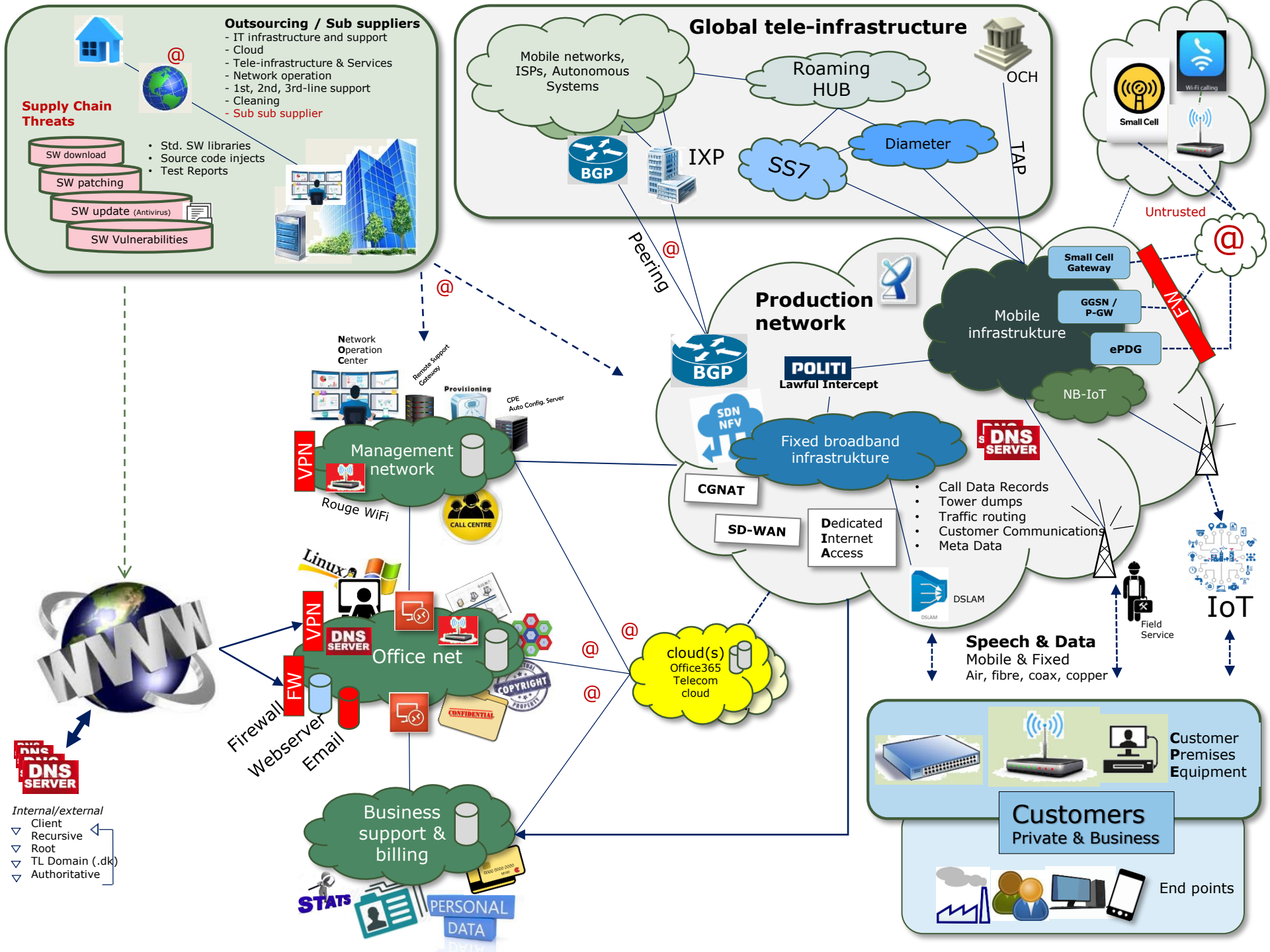
Wir hoffen, Ihr Anliegen zufriedenstellend bearbeitet zu haben und wünschen Ihnen eine gute Verbindung!

Mit freundlichen Grüßen

Ihr Kundenservice der Netcom Kassel

Bei Fragen und Anregungen können Sie uns unter folgenden Kontaktdaten erreichen:
Telefon: 0561 / 920 20 20 (montags bis freitags in der Zeit von 8 - 20 Uhr, samstags in der Zeit von 10 - 15 Uhr)
Fax: 0561 / 920 20 30
Internet: http://www.netcom-kassel.de
E-Mail: kundenservice@netcom-kassel.de

Dieses Schreiben wurde maschinell erstellt und ist ohne Unterschrift gültig.


Outsourcing / Sub suppliers
- IT infrastructure and support
- Cloud
- Tele-infrastructure & Services
- Network operation
- 1st, 2nd, 3rd-line support
- Cleaning
- Sub sub supplier
Supply Chain Threats
SW download
SW patching
SW update (Antivirus)
SW Vulnerabilities
• Std. SW libraries
• Source code injects
• Test Reports
Global tele-infrastructure
Mobile networks, ISPs, Autonomous Systems
Roaming HUB
OCH
BGP
IXP
SS7
Diameter
TAP
Small Cell
Wi-Fi calling
Untrusted
Peering
Production network
Mobile infrastrukture
Small Cell Gateway
GGSN / P-GW
ePDG
FW
NB-IoT
POLITI
Lawful Intercept
SDN NFV
Fixed broadband infrastrukture
DNS SERVER
CGNAT
SD-WAN
Dedicated Internet Access
• Call Data Records
• Tower dumps
• Traffic routing
• Customer Communications
• Meta Data
DSLAM
Field Service
IoT
Speech & Data
Mobile & Fixed
Air, fibre, coax, copper
Network Operation Center
Remote Support Gateway
Provisioning
CPE Auto Config. Server
Management network
VPN
Rouge WiFi
CALL CENTRE
Linux
Office net
VPN
DNS SERVER
FW
Firewall
Webserver
Email
COPYRIGHT
CONFIDENTIAL
cloud(s)
Office365
Telecom cloud
WWW
DNS SERVER
Internal/external
Client
Recursive
Root
TL Domain (.dk)
Authoritative
Business support & billing
STATS
PERSONAL DATA
Customer Premises Equipment
Customers
Private & Business
End points

GlobalConnect ramt af ransomware-angreb: Har spredt sig til flere af selskabets kunder

"Spain's fourth largest telecom operator hit by Revil ransomware gang!"

Spanish telecom giant MasMovil hit by Revil

Ransomware Attackers Demand Millions from Telecom Argentina

Telefonica, other Spanish firms hit in "ransomware" attack

EDITORS' PICK | Jul 17, 2020, 08:44am EDT | 20.578 views

Orange, Europe's Fourth-Largest Mobile Operator, Confirms Ransomware Attack

Home > N

Ecuador's state-run CNT telco hit by RansomEXX ransomware

By Lawrence Abrams

July 17, 2021 09:53 AM

CENTRE FOR CYBER SECURITY

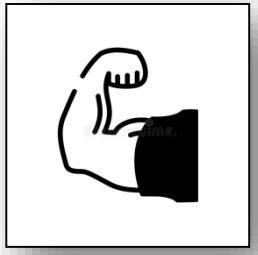
Impact on telecoms from ransomware

- Office network down
- No remote access to management network
- No access to tools or data
- Office phones not working
- Customers do not have access to support
- Customers do not have access to self-service portals
- Data theft and leak

👍 Mobile- and fixed internet services are still working

CENTRE FOR CYBER SECURITY

What makes the telecoms infrastructure robust?



- Logical separated from the internet and office network
- No mail clients and no direct remote access (?)
- Proprietary Linux / Unix based operation system
- Software upload protected by digital signature
- Password required to configure critical infrastructure
- The management network is not that critical

- Hackers prefer the low-hanging fruits
- Anything else?

CENTRE FOR CYBER SECURITY

Risks

- Poor separation between office network and management network
- Windows OS in telecoms infrastructure
- Ransomware targeting Linux / Unix (non-Windows OS)
- Mail-clients in the management network
- Remote connections to telecoms infrastructure (management and support)

- Virtualized telecom infrastructure running on COTS servers
- Ransomware targeting hypervisors
- Outsourcing (IT-hosting, Cloud, Support, Managed service)
- 5G native cloud core
- Open RAN
- Supply chain attacks
- Digital concentration

A recently-concluded investigation into a ransomware attack revealed that the attackers executed a custom Python script on the target's virtual machine hypervisor to encrypt all the virtual disks, taking the organization's VMs offline.

New Kubernetes malware backdoors clusters via Windows containers

Questions or remarks?

Mail: jenogg@cfcs.dk

CENTRE FOR CYBER SECURITY
Kastellet 30 / Holsteinsgade 63
2100 København Ø

Telefon: +45 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk