Cyber-Security im Krankenhaus

BPN – Cyber Security Partner der VAMED

bpn-group.com

Agenda

01 **Bedrohungslandschaft in Deutschland**
Gefahr oder Panikmache?

02 **Wer wird zum Ziel?**
Integrity, Availability & Insider Threat

03 **Was ist zu tun?**
Vorsorge – Reaktion

Bedrohungslandschaft in Deutschland

Gefahr oder Panikmache?

bpn-group.com

BBC

North Korea 'hackers steal US-South Korea war plans'

10 October 2017

The New York Times

MAY 14, 2017

Russia, This Time the Victim of a Cyberattack, Voices Outrage

CNN

Why the world should worry about North Korea's cyber weapons

October 11, 2017

The Economist

Can the American election be hacked?

Oct 26th 2016

Findet sich Deutschland überhaupt im Fokus der Cyberkriminalität?

cybermap.kaspersky.com/#

Frankfurter Allgemeine

Krankenhäuser sind ungeschützt gegen Hackerangriffe

30. November 2016

Frankfurter Allgemeine

Weltweite Attacke

„Das ist nicht vorbei“

„[…]Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes […] je nachdem, welcher der Beträge höher ist.“

Art. 83 Abs. 5 EU-DSGVO

WELT N24

Cyber-Attacke schleudert Klinik in 90er-Jahre zurück

12.02.2016

Frankfurter Allgemeine

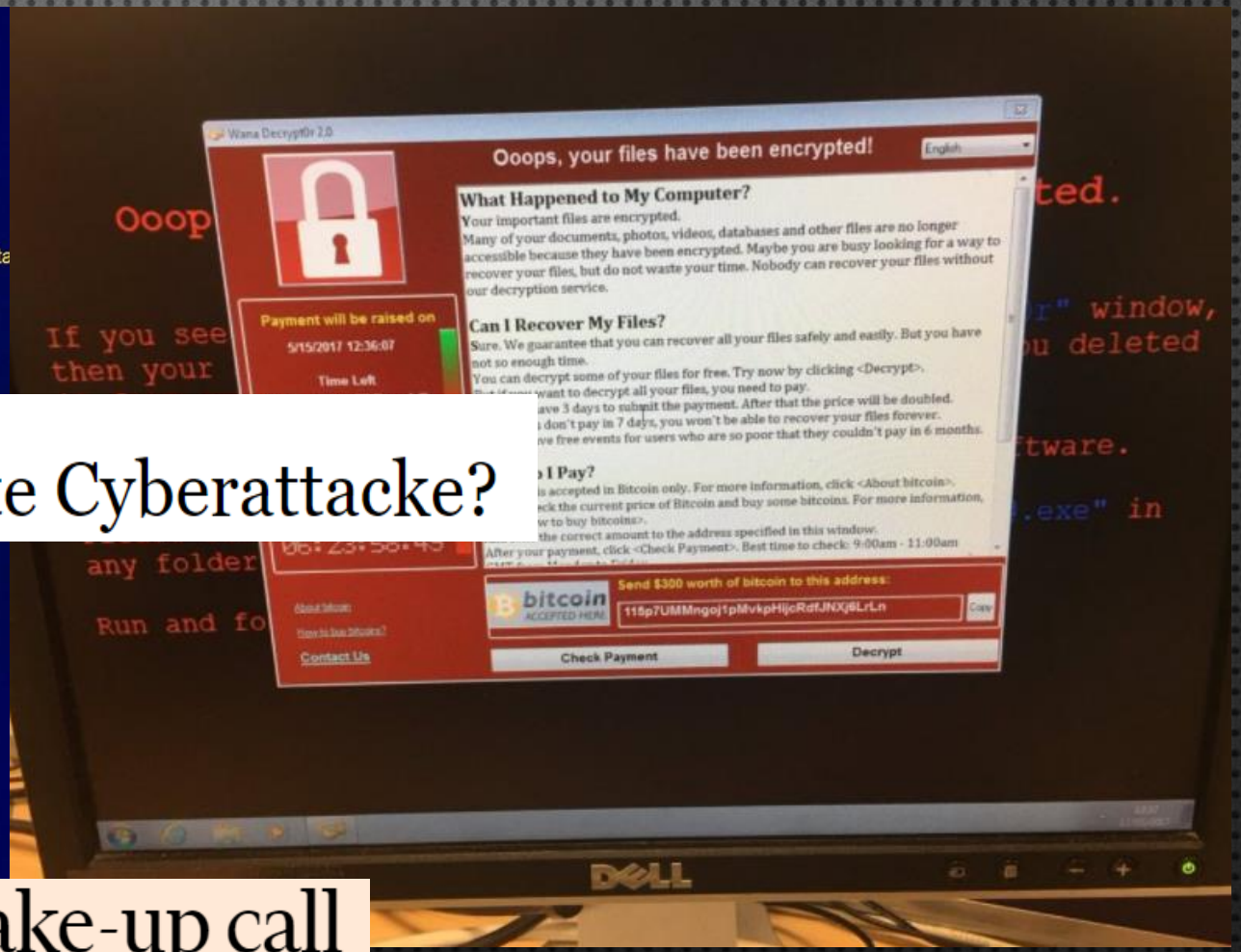
WELTWEITE ATTACKE

12.05.2017

Cyberattacke legt Krankenhäuser lahm

THE WALL STREET JOURNAL.

International Cyberattack Affects Some Corners of U.S. Health Care, Including Medical Devices



Frankfurter Allgemeine

Nach dem „Wanna Cry"-Angriff

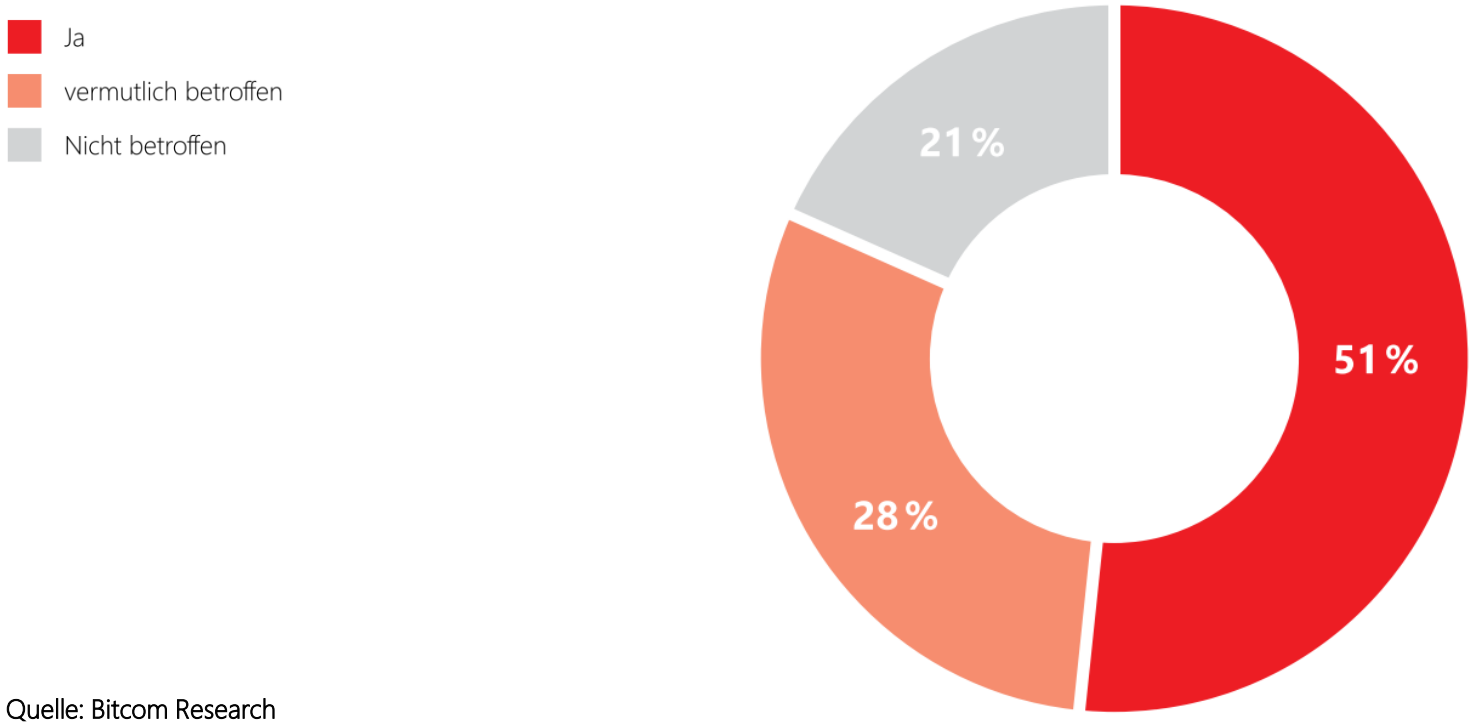
Droht eine zweite Cyberattacke?

FINANCIAL TIMES

The WannaCry attack is a wake-up call

Bedrohungslandschaft in Deutschland

Wurden Sie in den letzten beiden Jahren Opfer von Diebstahl, Spionage oder Sabotage?

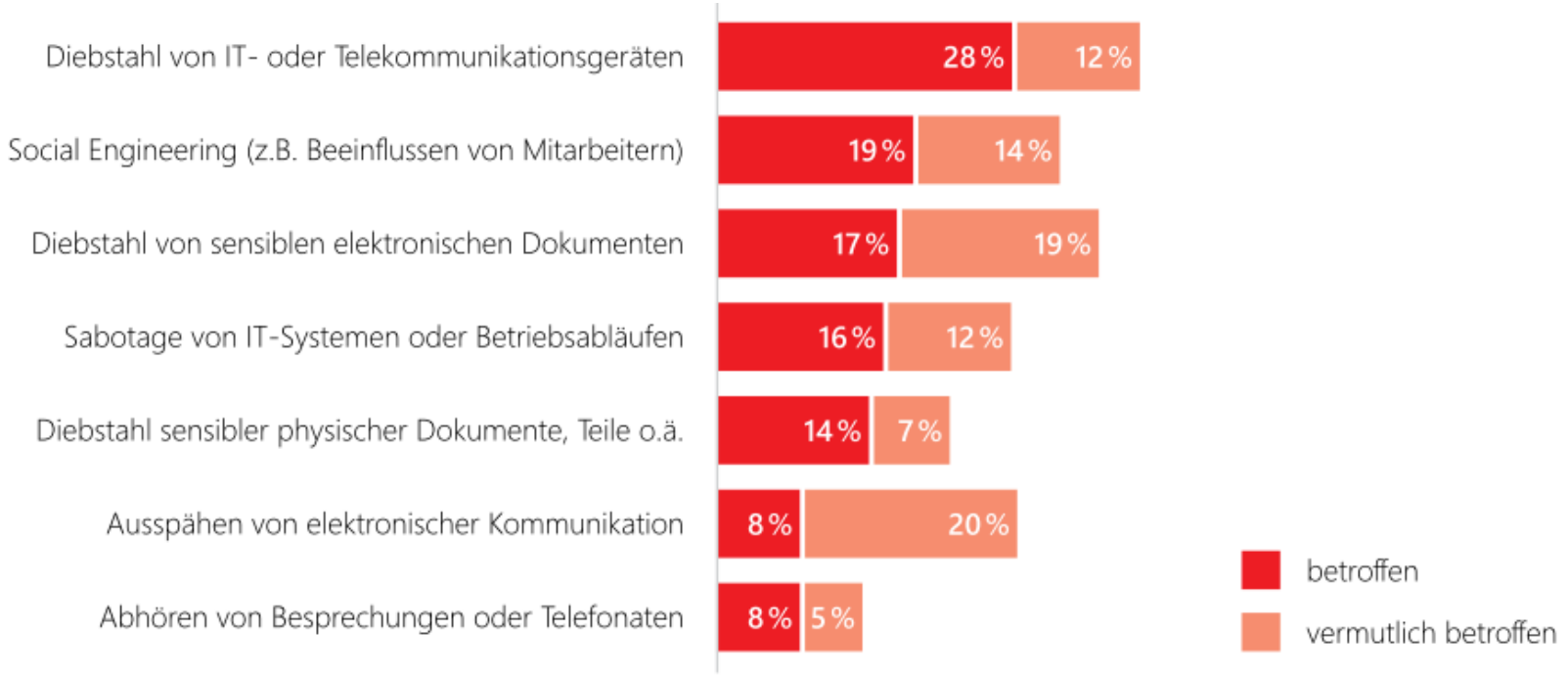


Quelle: Bitcom Research

Basis: Alle befragten Unternehmen (N=1.074)

Bedrohungslandschaft in Deutschland

Arten von Angriffen



Quelle: Bitcom Research

Basis: Alle befragten Unternehmen (N=1.074)

Wer wird zum Ziel?

Integrity, Availability & Insider Threat

Sind auch wir betroffen?

„Wir haben keine geheimen Daten…“

„Unsere Daten kann ruhig jeder sehen…“

„Was soll in einem Krankenhaus schon zu holen sein?“

Wer wird zum Ziel?

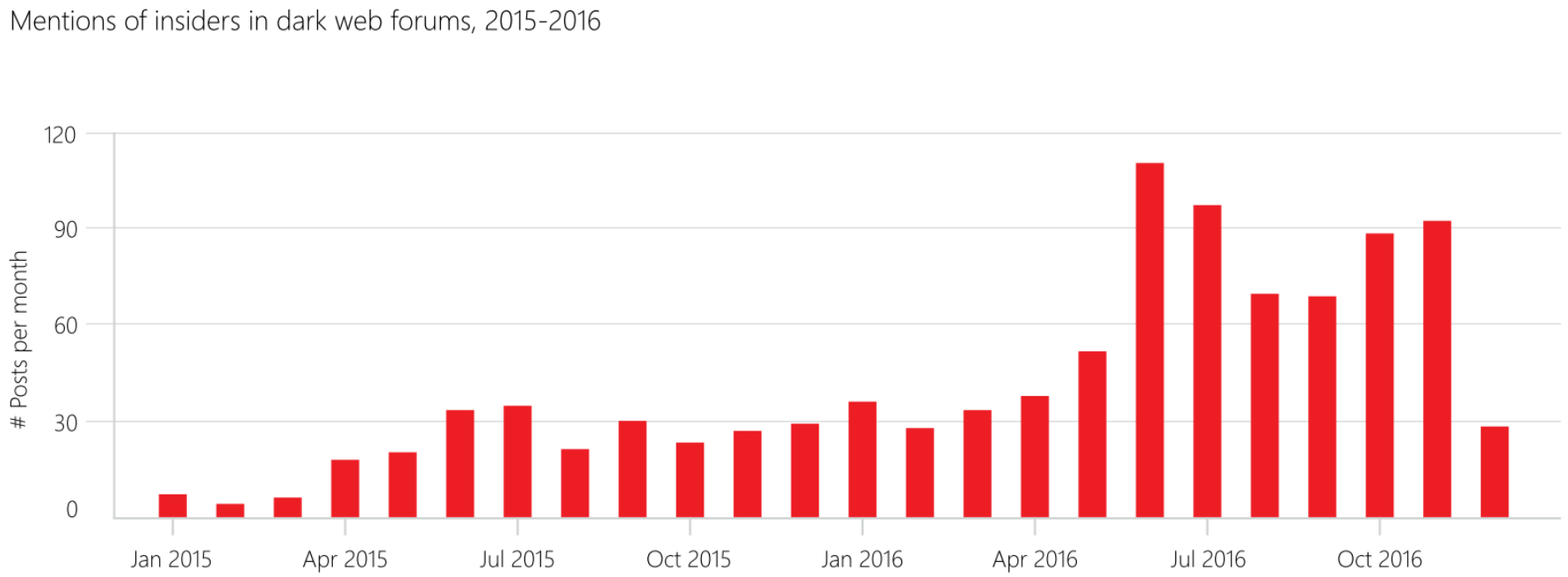
Sind wir auch betroffen?

Integrity vs. Availability

Insider Threat

Wer wird zum Ziel?

Insider Threat



Monetizing the Insider: The Growing Symbiosis of Insiders and the Dark Web

REDOWL, IntSights

Wer wird zum Ziel?

Insider Threat

Verlängerter Arm des Hackers

- Kick-Ass Marketplace - 35.800$ pro Woche Umsatz
- Zugang zu Insider Informationen für einen Bitcoin pro Monat (ca. 4.000 EUR)
- Platzieren von Malware unter Einsatz von Insidern

Monetizing the Insider: The Growing Symbiosis of Insiders and the Dark Web

REDOWL, IntSights

Was ist zu tun?

Vorsorge – Reaktion

Was ist zu tun?

Ausgangssituation

- Bedrohung von innen und außen!
- Ständige Veränderung der Angriffsvektoren!

VORSORGE

REAKTION

Prüfung
der Anfälligkeit gegenüber täglichen, realen Gefahren

Simulierte
strukturierte Angriffe auf kritische Assets (on- & offline)

Umfassenden Blick
auf die Resilienz Ihres Unternehmens

Identifizierung
Evaluierung und Minderung Ihrer Risiken
auf allen Ebenen

Konzeptionierung
von maßgeschneiderten Lösungen & Maßnahmen

Unterstützung
bei der Umsetzung & Adaptierung v. Konzepten

Einführung
von neuen Lösungen und Services

Optional
Outsourcing Leistungen
& Managed Security Services

Was ist zu tun?

Cyber Security HealthCare

DETECT 1	DETECT 2	SAP SCAN	TEST	REPORT	CONSULT	SUPPORT	MAINTAIN
Vulnerability Scan	Threat & Hacker-Hunting	SAP Vulnerability Scan	Targeted Cyber Attack	Outcome & Findings	Consulting & Solutions	Install & Implement	Support & MSP
Vulnerability Assessment – Schwach-stellenprüfung auf Hosts – Patch Management	Prüfung des Netzwerks auf – bestehende Infiltrationen & Schadsoftware – Zugriffe durch Hacker – Ausspähung der Infrastruktur durch Hacker	Prüfung der SAP Infrastruktur auf – Sicherheitsge-fährdende Konfigurations-änderungen – Missbrauch von Passwörtern & Administrativen Zugängen – Möglichkeit von SQL-Angriffen – Missbrauch von Web-APIs	Targeted Cyber-Angriff (Blackbox) – Simulation eines realen Hackerangriffes – Testen der Angriffs-möglichkeiten – Ist es möglich, kritische Geräte zu übernehmen?	Auswertung durchgeführter Module – Präsentation – Aufbereitung der Findings – Ausblick auf notwendige Maßnahmen	Erstellung Maßnahmen-katalog – Konzept – Abwehr- und Schutzmecha-nismen – Lösungen für offengelegte Schwachstellen	Implementierung & Installation Schutz-maßnahmen – Umsetzung Verbesserungs-maßnahmen – Installation Schutzmaßnah men	Managed Security, Services & Maintenance – Fortlaufende Wartung & Unterstützung – Security Reviews

Was ist zu tun?

SAP Vulnerability Scan

SAP SCAN

SAP Vulnerability Scan

Prüfung der SAP Infrastruktur auf

- Sicherheitsgefährdende Konfigurationsänderungen
- Missbrauch von Passwörtern & Administrativen Zugängen
- Möglichkeit von SQL-Angriffen
- Missbrauch von Web-APIs

Authorisierungs-managementt	Ist die Rollenverteilung im System kongruent mit bestehenden Policies?
Konfiguration	Wurden entsprechende Sicherheitseinstellungen gesetzt oder Voreinstellungen verändert?
Anmeldungs-versuche	Ist eine Anmeldung mittels abgelaufener, gelöschter oder gesperrter Konten möglich? Gelingt ein missbräuchlicher Zugang über Standard-Benutzerkonten?
Kritische Transaktionen	Black- und Whitelists: Sind verbotene/gesperrte Transaktionen, Reports oder Module ausführbar?
Remote-Zugriffe	Gelingt der Zugriff nicht-produktiver Systeme auf Produktionssysteme mittels System Calls?
Debugging / Fehleranalyse	Wird sichergestellt, dass kein Missbrauch von Debuggern in Produktionssystemen vorkommt?
Denial of Service	Werden Anzeichen einer Systemüberforderung erkannt, die zu verlangsamter Reaktion oder sogar zum vollständigen Ausfall führen kann?
Web-APIs	Ist ein Missbrauch von Web-APIs möglich, um sich Zugang zu verschaffen?
Administrator-Zugänge	Wie wird eine Manipulation von Administrator-Passwörtern verhindert?
SQL-Funktionen	Werden verdächtige Zugriffe von SQL-Funktionen im System erkannt?
Muster-erkennung	Erfolgt eine Erkennung spezifischer Verhaltensmuster, die auf einen Angriffsversuch hinweisen?

REPORT

Outcome & Findings

Auswertung & Visualisierung

- Überblick über SAP-Umgebung
- Möglichkeit der Auswertung in Real Time aufzeigen
- Grundlage für weiteren Vertrieb ETD


BPN
office@bpn-group.com
bpn-group.com