RADAR SERVICES

Cyber Risiken – Tatsächliche Gefahr für die deutsche Wirtschaft oder nur ein weiterer Hype?

Wie man IT-Sicherheitsrisiken gezielt erkennt und sich erfolgreich gegen den ungewollten Datendiebstahl schützt

Sebastian Michels
Head of Partner Sales, Miteigentümer RadarServices

500 | Technology Fast 500 2016 EMEA WINNER Deloitte.

IT Security made in Europe

ECS EUROPEAN CYBER SECURITY ORGANISATION

Teilnehmer der Allianz für Cyber-Sicherheit

Nur ein paar Beispiele von Cyber Attacken und deren mögliche Ausprägungen…

UMFANGREICHE DDOS ATTACKEN

BBC Sign in News Sport Weather

NEWS

Home Video World UK Business Tech Science Magaz

Technology

Cyber attack takes down Dutch government sites

12 February 2015 | Technology

A cyber-attack took down most of the Dutch government's webs Tuesday, it has been confirmed.

The attack, which also took down some private sites, highlighted the of public infrastructure.

HELP NET SECU

NEWS MALWARE ARTICLES R

ibe for free

e archive

19,000 French websites hit by DD wake of terror attack

Posted on 16 January 2015.

Since the three day terror attack that started in Fra the attack on satirical newspaper Charlie Hebdo, 1 French-based companies have been targeted by c reports.

According to Admiral Arnaud Coustilliere, the Fren cyberdefense, most of these attacks were carried hacker groups: Middle East Cyber Army, Fallaga t Caliphate.

This unprecedented avalanche of cyber attacks tar sites and that of big and small businesses. Most w attacks, and some were web defacements.

In a report published on Wednesday, Radware Islamic hacker group AnonGhost has also launche France.

"Over the last few days, AnonGhost has brought d websites, replacing the pages with a manifesto an images," they shared.

World's largest DDoS attack reached 400Gbps, says Arbor Networks

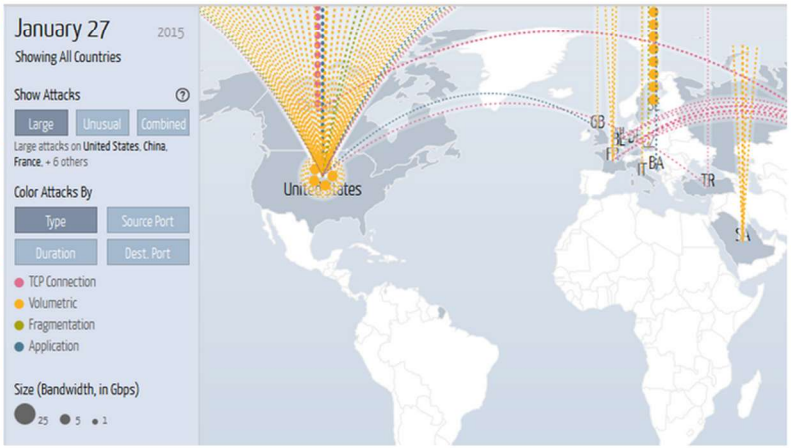
NTP amplification fuelling era of super-massive DDoS

By John E Dunn | Jan 27, 2015

Share

Some time in December 2014 an unnamed ISP experienced an NTP reflection DDoS attack that peaked at a router-straining 400Gbps, easily the largest denial of service event in Internet history, Arbor Networks' 10th Annual Infrastructure Report has revealed.

It's an apparently small detail slipped into the firm's larger narrative which is probably less important in the grand scheme of things than the fact that super-massive DDoS attacks are now common enough to have turned into dull statistics.

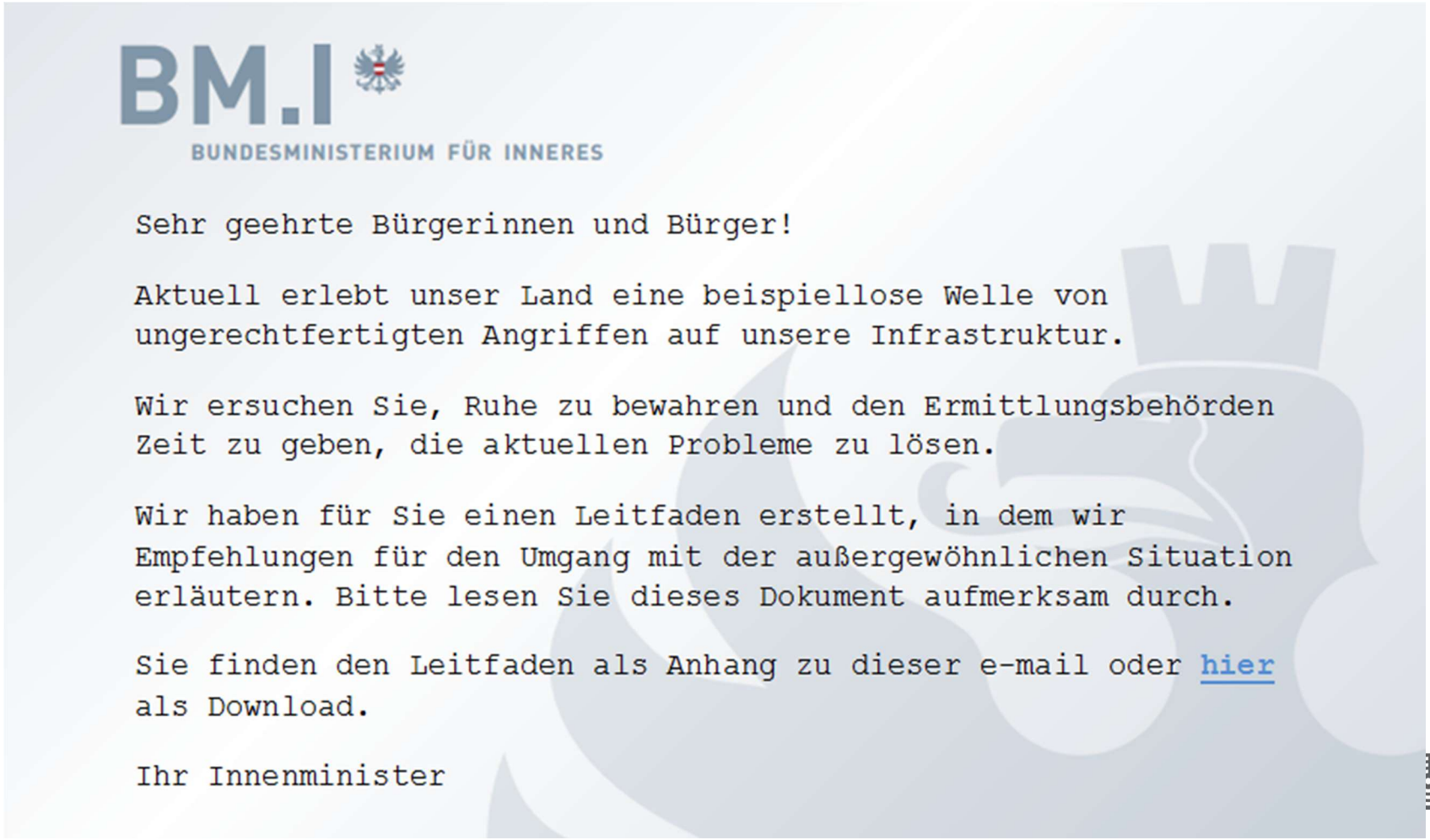


Message - large DDoS attacks are here to stay. But what is driving this ballooning traffic?

DEFACEMENT

RADAR SERVICES

MASSIVE MALWARE VERTEILUNG



BM.I

BUNDESMINISTERIUM FÜR INNERES

Sehr geehrte Bürgerinnen und Bürger!

Aktuell erlebt unser Land eine beispiellose Welle von ungerechtfertigten Angriffen auf unsere Infrastruktur.

Wir ersuchen Sie, Ruhe zu bewahren und den Ermittlungsbehörden Zeit zu geben, die aktuellen Probleme zu lösen.

Wir haben für Sie einen Leitfaden erstellt, in dem wir Empfehlungen für den Umgang mit der außergewöhnlichen Situation erläutern. Bitte lesen Sie dieses Dokument aufmerksam durch.

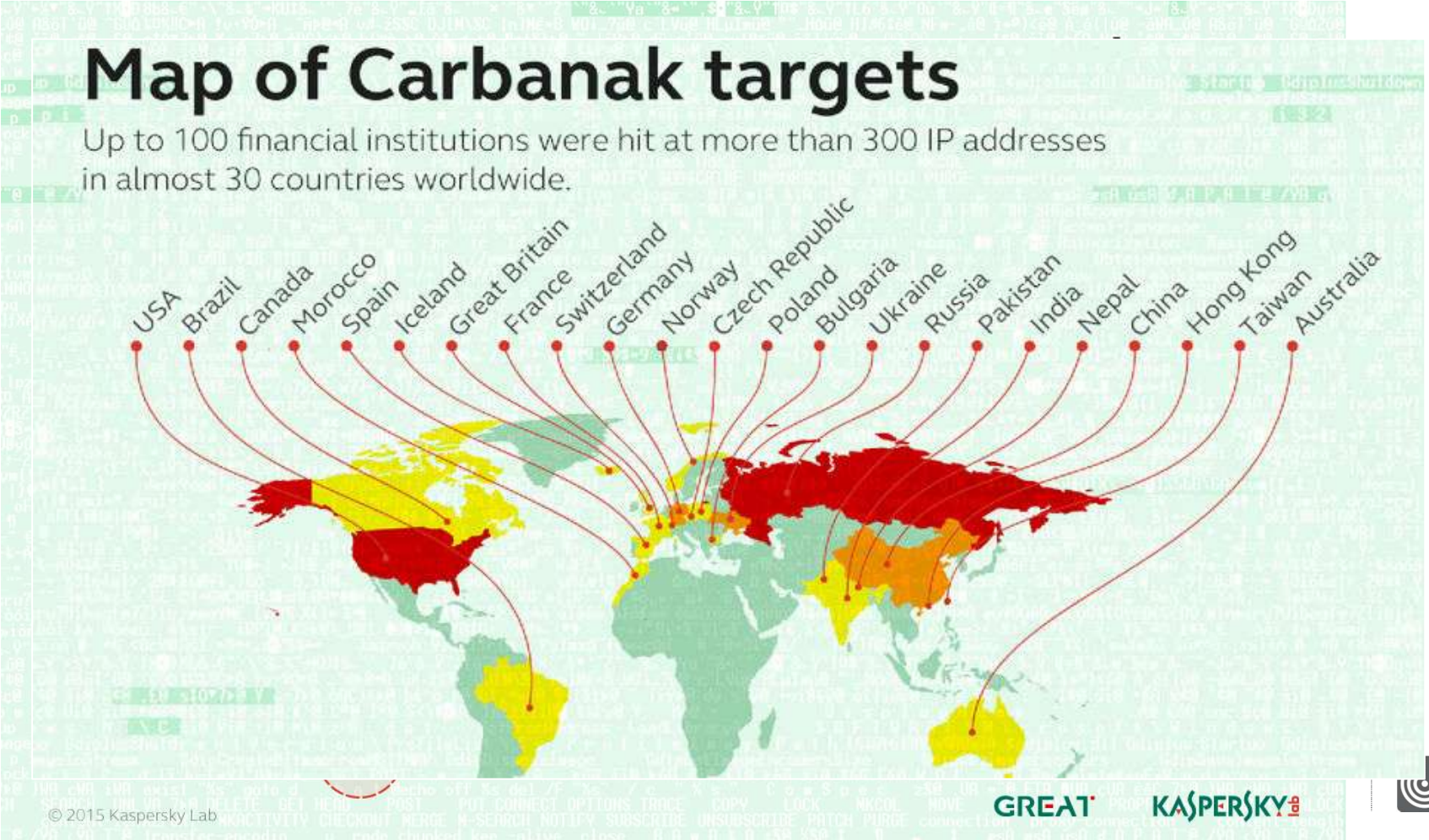
Sie finden den Leitfaden als Anhang zu dieser e-mail oder hier als Download.

Ihr Innenminister

RADAR SERVICES

Wer von Ihnen hat im privaten- oder auch in ihrem Unternehmensumfeld von Cyber Vorfällen gehört??

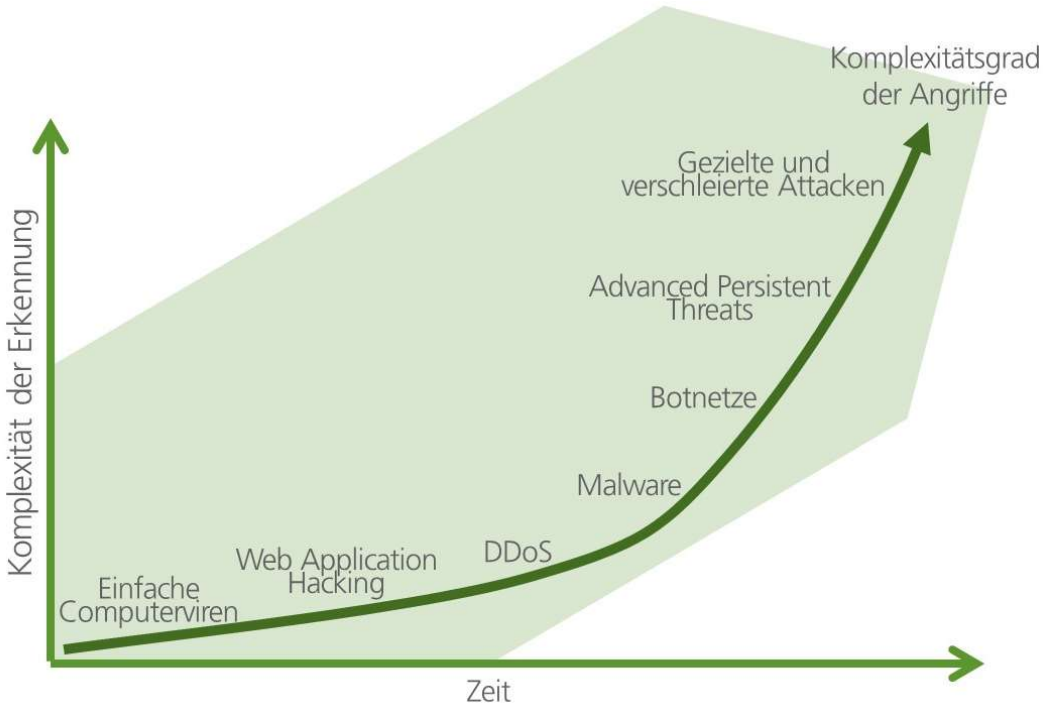
ANGRIFFE AUF BANKOMATEN



RADAR SERVICES

Sabotage, Wirtschaftskriminalität und CyberCrime und die weltweiten Schäden – Warum funktioniert das so einfach und gut?

Wachsende Bedrohungen



Frankfurter Allgemeine
Wirtschaft
Mittwoch, 04. November 2015

Wirtschaftsspionage

Unternehmen schützen sich zu wenig vor der NSA

Geheimdienste wie die amerikanische NSA haben die Wirtschaft im Visier. Die getroffenen Sicherheitsmaßnahmen der Unternehmen sind unzureichend. Sie zu umgehen – ein leichtes Spiel.

ZDNet / Sicherheit / Virus

Computerviren legen Systeme mehrerer Kliniken in NRW lahm

von Björn Greif am 12. Februar 2016, 10:48 Uhr

Mehrere Kliniken in Nordrhein-Westfalen sind in jüngerer Vergangenheit Computerviren z Opfer gefallen. Neuester Fall ist der des Lukaskrankenhauses in Neuss, dessen Systeme einen vorschnell geöffneten E-Mail-Anhang infiziert wurden. Nach Informationen von RP waren zuvor auch Kliniken in Essen, Köln und Mönchengladbach von ähnlichen Vorfälle betroffen.

ZEIT ONLINE

Wirtschaftsspionage

"Ein gnadenloser Krieg"

Der französische Geheimdienst schnüffelt ganz offiziell im Namen der Nation für seine Unternehmen – und eine eigens gegründete Schule lehrt den Beruf Wirtschaftsspion.

SPIEGEL ONLINE POLITIK

Abhör-Affäre: BND-Mitarbeiter erhärtet Verdacht auf Wirtschaftsspionage

In der NSA-Affäre sind weitere Indizien dafür aufgetaucht, dass der US-Geheimdienst deutsche Unternehmen ausgeforscht hat. Nach Informationen des SPIEGEL kannte ein BND-Mitarbeiter Suchbegriffe mit deutschen Firmennamen.

RADAR SERVICES

Vernetzt – Komplex – Überall

1 Technologische Durchdringung und Vernetzung: Alle physischen Systeme werden von IT erfasst und schrittweise mit dem Internet verbunden.

Quelle: BSI.de

RADAR SERVICES

Vernetzt – Komplex – Überall

2 Komplexität: Die Komplexität der IT nimmt durch vertikale und horizontale Integration in die Wertschöpfungs-prozesse erheblich zu.

Quelle: BSI.de

RADAR SERVICES

Vernetzt – Komplex – Überall

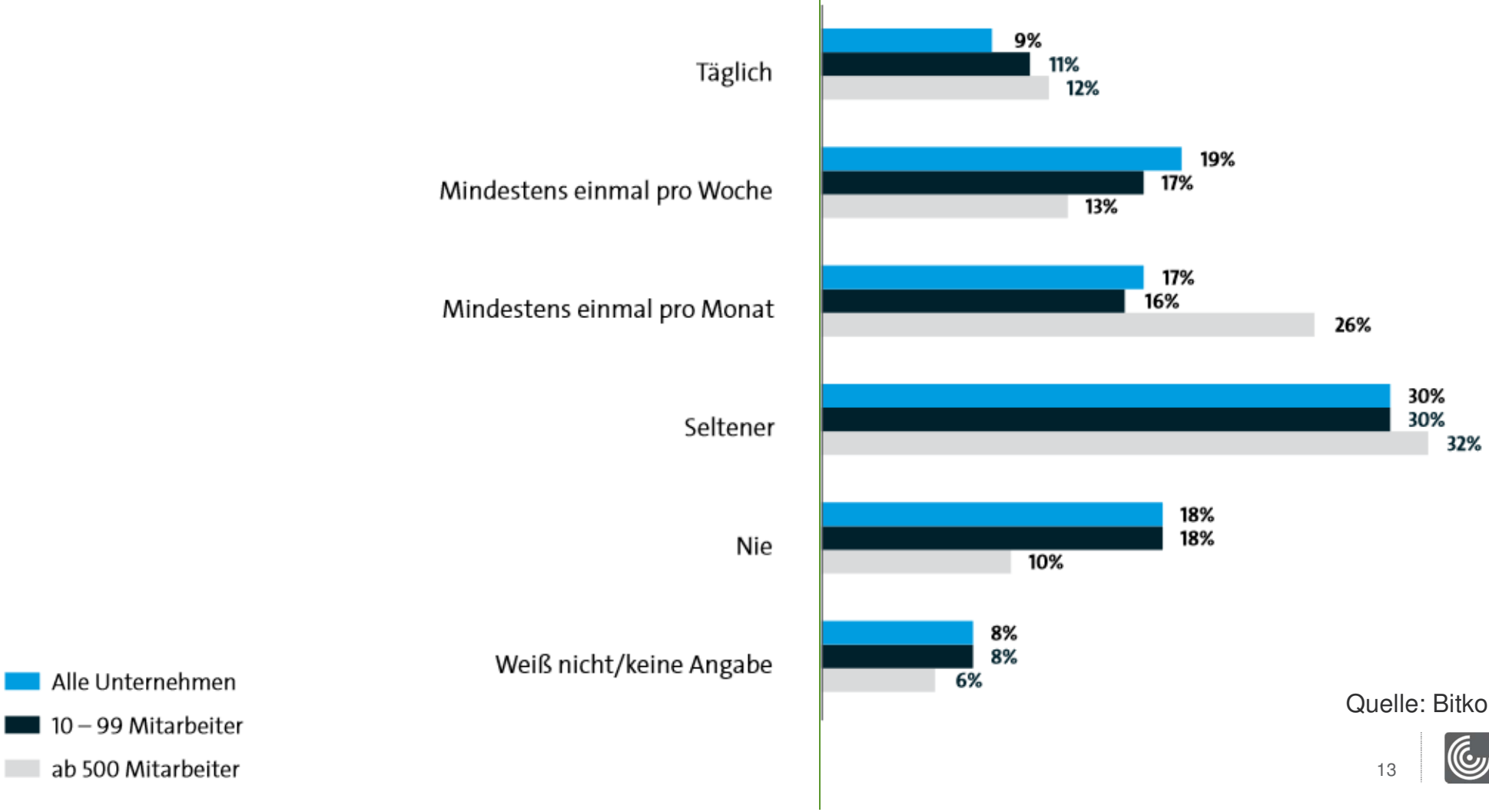
3 Allgegenwärtigkeit: Jedes System ist praktisch zu jeder Zeit und von jedem Ort über das Internet erreichbar.

Quelle: BSI.de

RADAR SERVICES

Häufigkeit der Angriffe

45% der Unternehmen verzeichnen monatlich **ernste** Angriffe



Quelle: Bitkom.de, n=1.074

RADAR SERVICES

Schadenssumme (Deutschland)

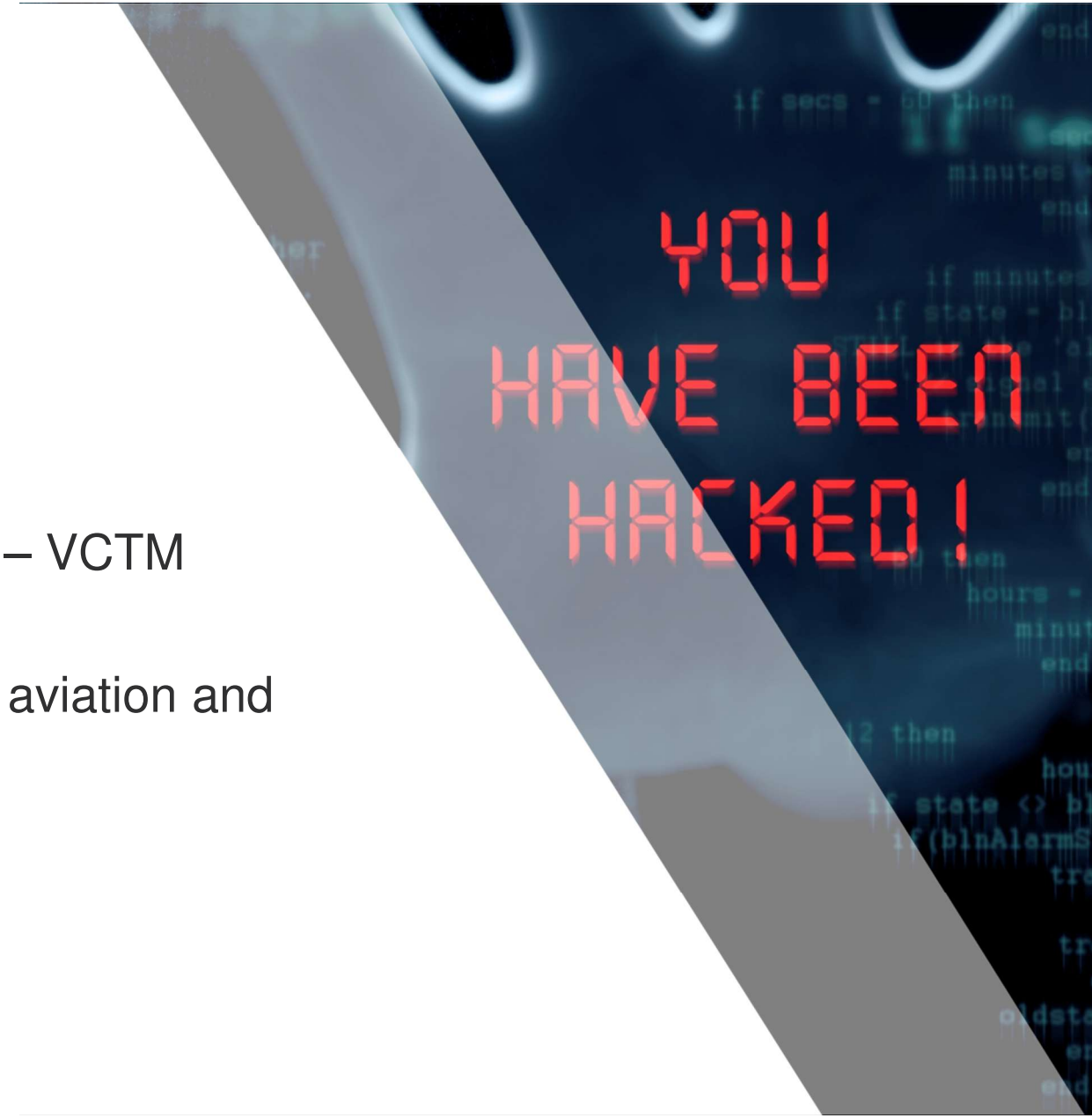
Delikttyp	Schadenssumme (in Euro)
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	23,0 Mrd.
Patentrechtsverletzungen (auch vor der Anmeldung)	18,8 Mrd.
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	14,3 Mrd.
Ausfall, Diebstahl oder Schädigung von IT-Systemen, Produktions- oder Betriebsabläufen	13,0 Mrd.
Imageschaden bei Kunden oder Lieferanten / Negative Medienberichterstattung	12,8 Mrd.
Kosten für Rechtsstreitigkeiten	11,8 Mrd.
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	3,9 Mrd.
Erpressung mit gestohlenen Daten	2,9 Mrd.
Höhere Mitarbeiterfluktuation / Abwerben von Mitarbeitern	1,7 Mrd.
Sonstige Schäden	0,2 Mrd.
Gesamtschaden innerhalb der letzten zwei Jahre	**102,4 Mrd.**

Quelle: Bitkom.de

Anatomy of a life changing Cyber attack.

VICTIMA Ltd.

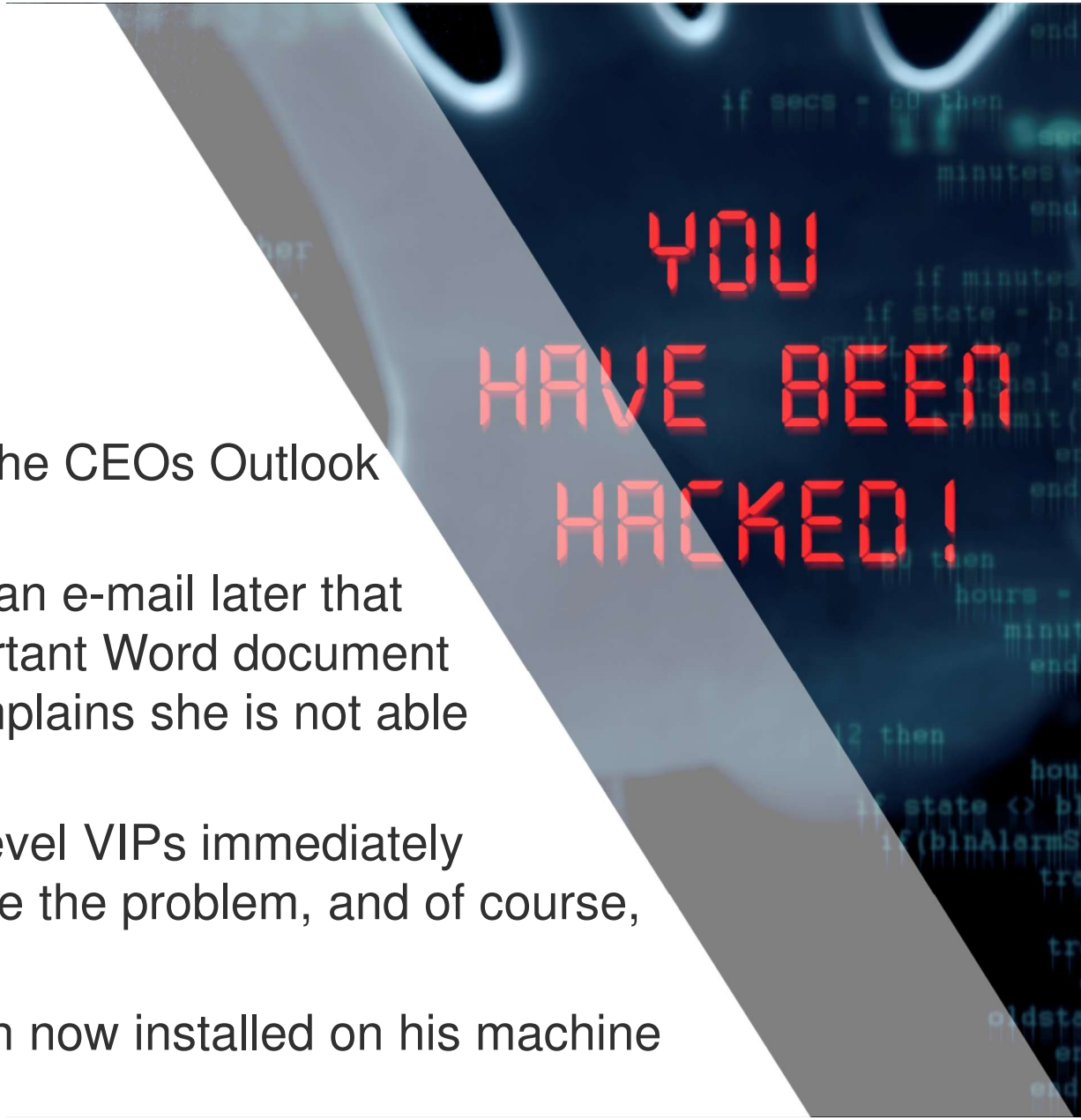
- 12,000 employees
- Headquartered in Hamburg
- Listed at Frankfurt Stock Exchange – VCTM
- Current share price: EUR 28,90
- Sub-contractor and key-supplier for aviation and automotive industry



DAY 1 - MONDAY

- Greta, the CEO‘s assistant, checks the boss‘ favorite restaurants website for todays menu
- The attacker already knew about the restaurant due to a facebook posting of the CEO after his latest dinner at the restaurant
- The website of the restaurant is using an outdated, vulnerable version of a content management system
- The attacker penetrates the website and plants a hidden virus-download into the site
- Greta, while doing here job, receives a nice gift from the website – a sophisticated malware

DAY 2 - TUESDAY



- The attacker has gained full remote control of Greta‘s PC
- Greta, of course, has full access to the CEOs Outlook (e-mail, calendar, contacts etc.)
- Greta (well, not really she…) sends an e-mail later that day to IT support, including an important Word document with an embedded macro Greta complains she is not able to open on her PC
- John from special IT support for C-level VIPs immediately opens the Word document to analyze the problem, and of course, he runs the macro…
- The macro is actually a hidden trojan now installed on his machine

DAY 3 - WEDNESDAY

- The malware on John‘s PC silently looks for his administrative-level credentials
- Before noon, the attacker has gained access to the central user management system and is able to create his own administrative accounts on core office and production control environments
- Using the newly generated accounts, the attacker spreads malware and remote control software throughout the primary production plants
- Put options of VCTM stock are purchased through anonymous channels in large scale

DAY 4 - THURSDAY

- A highly confidential e-mail of the CEO sent to the company‘s law firm gets leaked to selected journalists confirming a long expected take-over of a main competitor
- Unfortunately, neither Greta nor the CEO have ever written such an e-mail
- Several tweets and news websites report the rumors at the same time
- The stock price boosts and climbs to EUR 41,00 – investors are thrilled
- The CEO is denying reports of the planned take-over

DAY 5 – BLACK FRIDAY

- 7.45 AM: 65% of all production control systems stop functioning due to encrypted files and deleted user accounts
- 9.30 AM: a faked e-mail of the CEO is sent to press contacts, confirming a serious Cyber attack, eventually week long production problems and the threat of multi-million EUR fines for disrupting main contractor production lines
- 10.15 AM: thousands of Twitter feeds created by communication bots are spreading the information and confirming the fake news
- 2.40 PM: Stock price drops by more than 50% to EUR 19,50
- 3.55 PM: The attacker makes millions of EUR using the purchased put options
- 5.30 PM: VICTIMA is devastated – production offline – its image seriously damaged

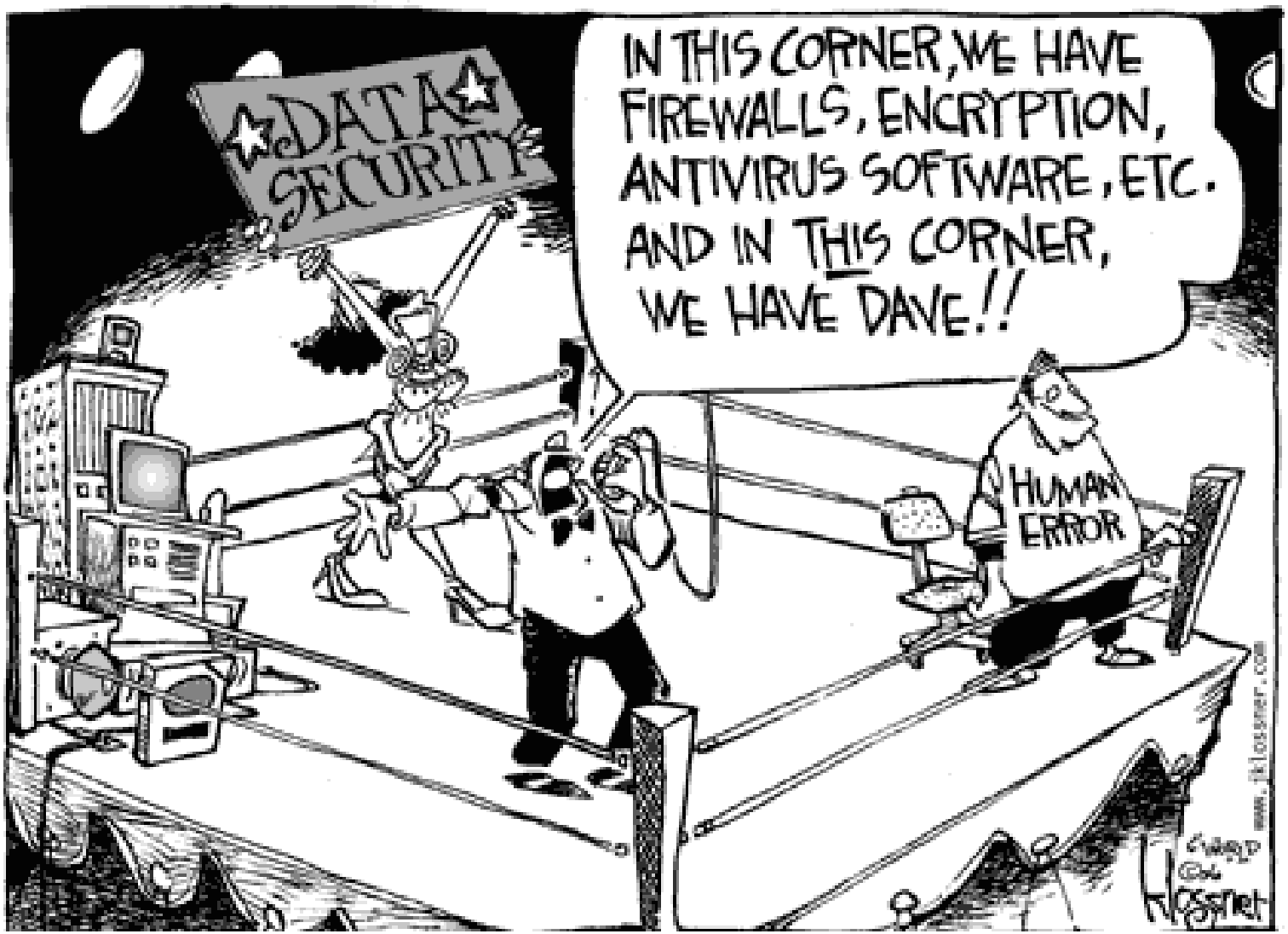
Halten Sie solche Cyber Attacken und Auswirkungen für möglich?

What needs to be done to become resilient?

Was also tun?

- IT abschalten?
- Zurück zum Mainframe?
- Mehr IT Schutzsysteme?
- Keine e-mail Anhänge oder Downloads mehr?
- Anwender vom PC fernhalten?

Die Realität.



RADAR SERVICES

Welche Maßnahmen müssten aus Ihrer Sicht ergriffen werden?

Strukturiertes Vorgehen erwünscht!

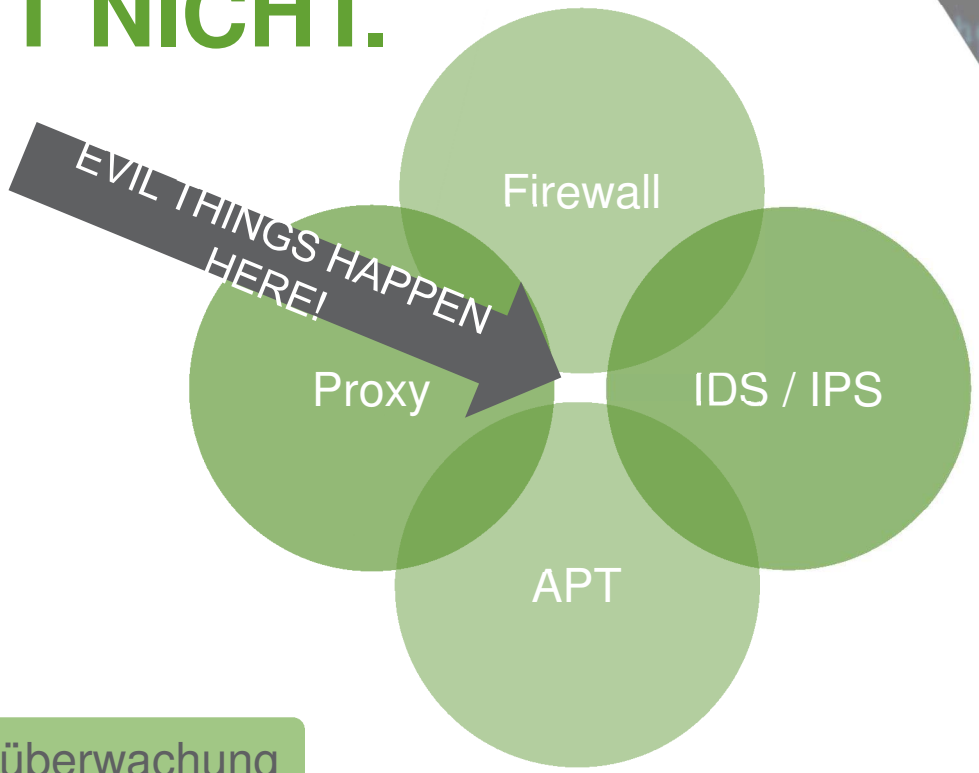
- Balance zwischen „Prevention“ und „Detection“ schaffen
- Schulung der Mitarbeiter
- Risikoakzeptanz-Entscheidungen durch die Geschäftsführung herbeiführen
- Die Kronjuwelen identifizieren
- Sicherheits-, Notfall-, Backup- und Wiederanlaufpläne schaffen
- Und üben!
- **Es ist nicht die Frage OB, sondern WANN…**

Aufbau eines Cyber Defense Centers – Eine Möglichkeit Sicherheitsrisiken frühzeitig zu erkennen?

KOMPLEXE HERAUSFORDERUNGEN.

- Wie erkenne ich moderne, gezielte Angriffsszenarien?
- Wie stelle ich Korrelation über Ereignisse oder Ereignisketten her?
- Wie bewerte ich das Risikopotential?
- Wie erhalte ich anwendbare Anleitungen für die Behandlung von Risiken?
- Wie wird überprüft, ob Verbesserungen erfolgreich waren?
- Wie gestalte ich einen effizienten Informationsfluss zu allen Beteiligten?
- Wie schaffe ich Risikotransparenz (vom IT- zu Geschäftsrisiko)?

TECHNOLOGIE ALLEIN
REICHT NICHT.



24/7 Systemüberwachung

24/7 Schutz vor bisher unbekannten Angriffsmustern

Pay-as-you-grow OPEX Model

DO BIGGER WALLS REALLY HELP?

- Should we really build more, bigger and thicker Security walls!
- Is it not more important to find security incidents in a shorter detection time?

RADAR SERVICES

MACHINE VERSUS
RADARSERVICES SOC.

NG Firewall IDS / IPS	APT – Sandboxing	RADARSERVICES SOC
Perimeterlogs PCAP – Analyse IPS Signaturen	Perimeterlogs PCAP – Analyse IPS Signaturen	Infrastrukturlogs Analysten Incident Reporting SOC Services
Erkennt: 5 Attacken	Erkennt: 12 Attacken	**Erkennt: 57 Attacken**
= 1Attacke in 14 Tagen / 7%	= 1 Attacke in 1 Woche / 18%	= 1 Attacke pro Tag / 75%

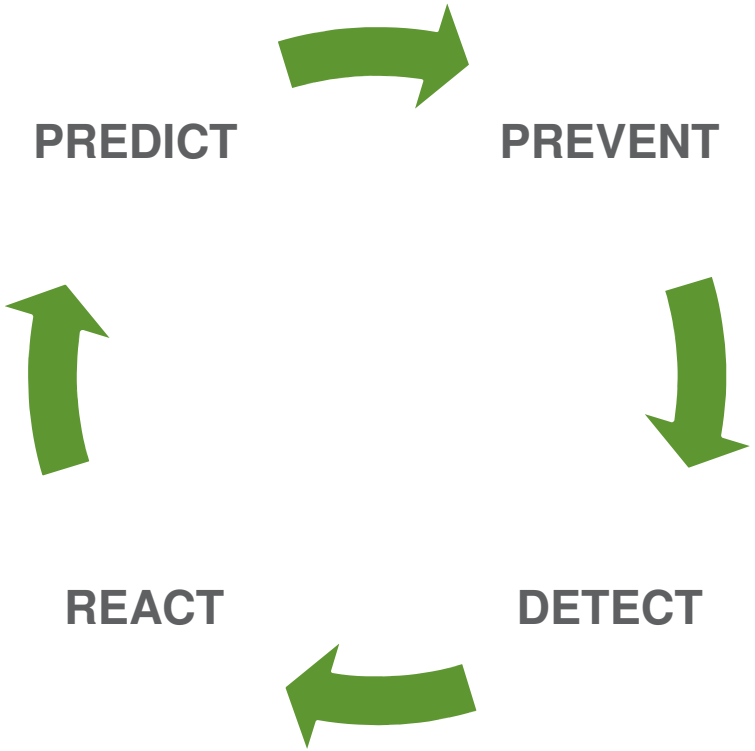
A Cyber Defense Center as Foundation of Comprehensive IT Risk Detection.

A CHANGE OF PARADIGM.
THE PREVENTION FAILURE.

PREVENT

RADAR SERVICES

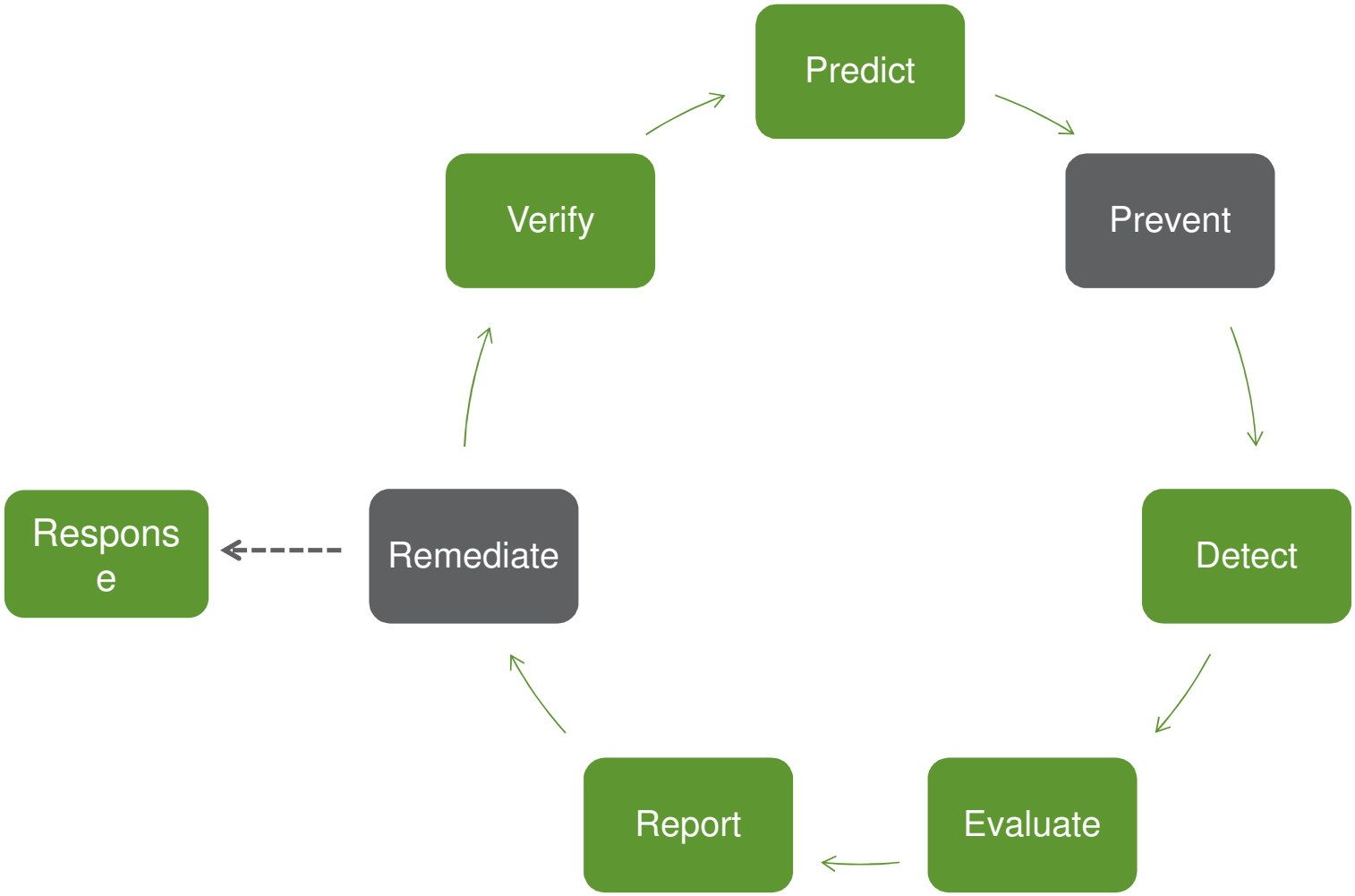
A CHANGE OF PARADIGM.
THE PREVENTION FAILURE.



RADAR SERVICES

Transforming a Cyber Defense Center into a Value Proposition.

PROCESSES.
IT RISK MANAGEMENT
WORKFLOW.



IT Operations
Cyber Defense Center

RADAR SERVICES

RADAR SERVICES

DIE NÄCHSTE WELLE KOMMT.

RadarServices –

das Frühwarnsystem für Ihre IT.

500 | Technology Fast 500 2016 EMEA WINNER Deloitte.

IT Security made in Europe

ECS EUROPEAN CYBER SECURITY ORGANISATION

Teilnehmer der Allianz für Cyber-Sicherheit

EUROPÄISCHE WURZELN,
WELTWEIT IM EINSATZ.

100% IT-SECURITY MADE IN EUROPE.

4 KONTINENTE, AUF DENEN WIR EINGESETZT WERDEN.

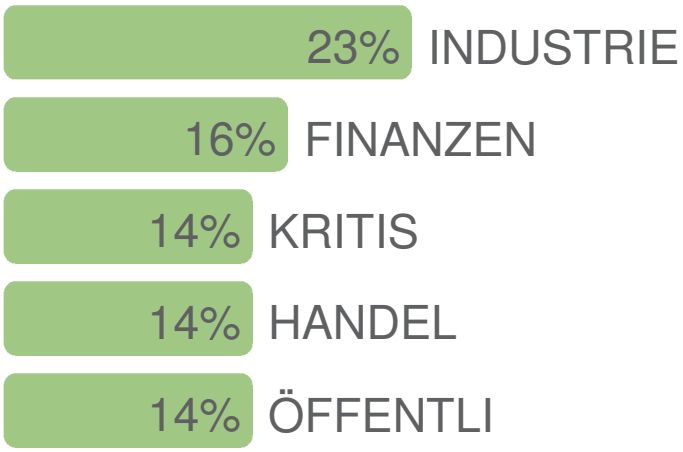
170 LÄNDER, IN DENEN UNSERE KUNDEN TÄTIG SIND.

120 MITARBEITER.

SOCs:	WIEN (HQ)	BERLIN	VADUZ	DUBAI
BÜROs:	FRANKFURT	WARSCHAU	MOSKAU	

MIT SICHERHEIT ERFOLGREICH: ÜBER UNSERE KUNDEN.

UNTERNEHMEN NACH BRANCHEN



UNTERNEHMEN NACH GRÖSSE (ANZ.

RADAR SERVICES

RadarServices ist einer von
Europas führender Anbieter
von Managed Security Services.

Im Mittelpunkt steht die
zeitnahe Erkennung von
IT-Sicherheitsvorfällen und -risiken.

WIEN: DAS GRÖSSTE SOC
IN EUROPA.

188 PETABYTE DATEN.

24 BILLIONEN EVENTS.

260 MILLIONEN SCHWACHSTELLENINFORMATIONEN.

1,6 MILLIONEN IDENTIFIZIERTE INCIDENTS.

TECHNOLOGIE:

- MEHRSTUFIGE KORRELATION
- BREITES SPEKTRUM AN EREIGNISSEN
- MACHINE LEARNING
- INTERNE ENTWICKLUNG

Durchschnittsangaben pro Jahr

DAS KOMPLETTPAKET:
WERKZEUGE, EXPERTEN, PROZESSE.

AUTOMATISIERTE RISIKOERKENNUNGS- MODULE

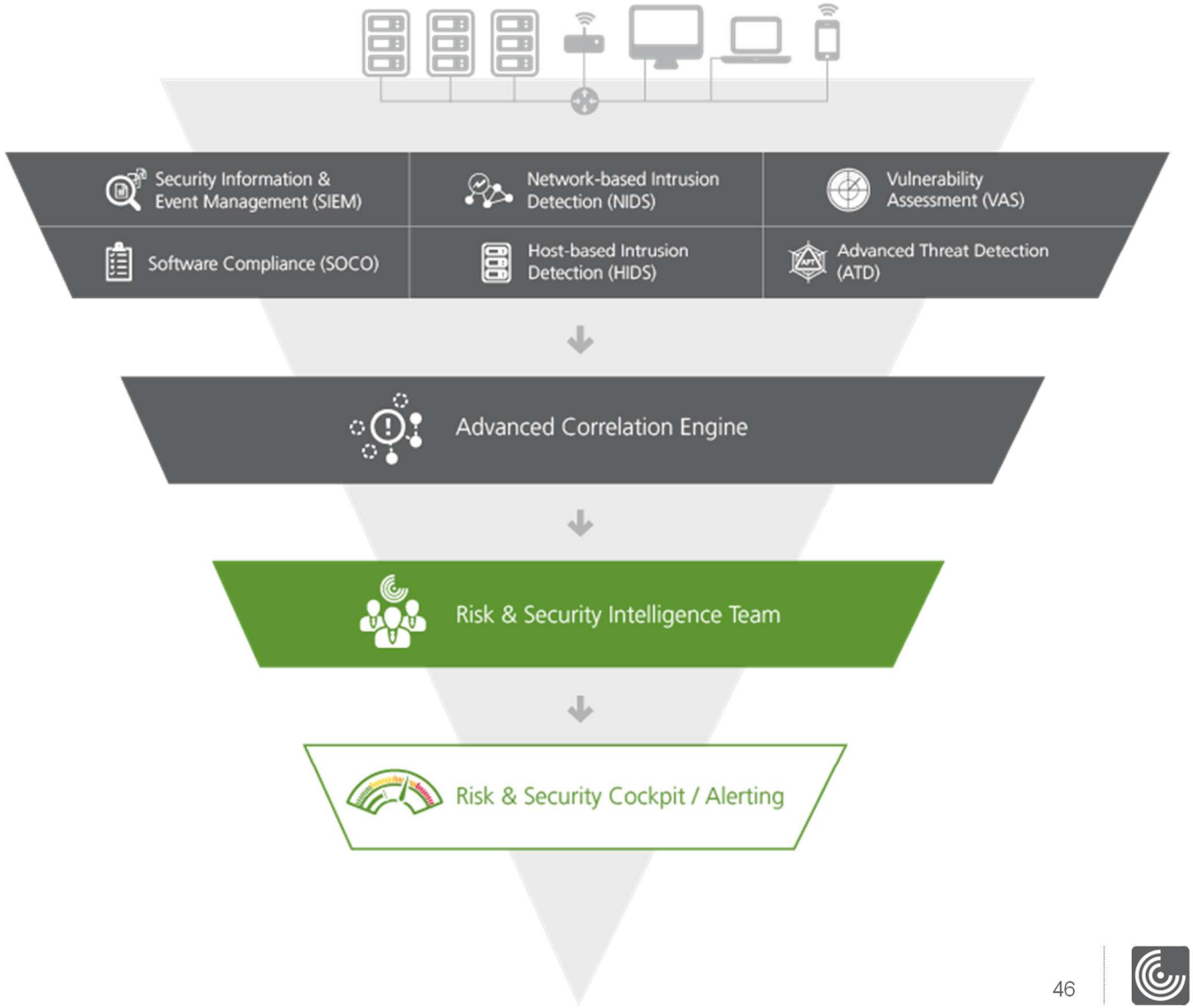
ADVANCED CORRELATION

RISK & SECURITY INTELLIGENCE TEAM

CUSTOMIZED REPORTS & ALARMIERUNG

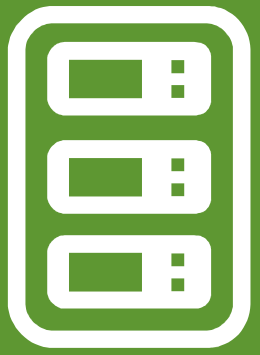
Mehrstufige Erkennung in modularer Architektur.

RADARSERVICES
DAS SYSTEM.



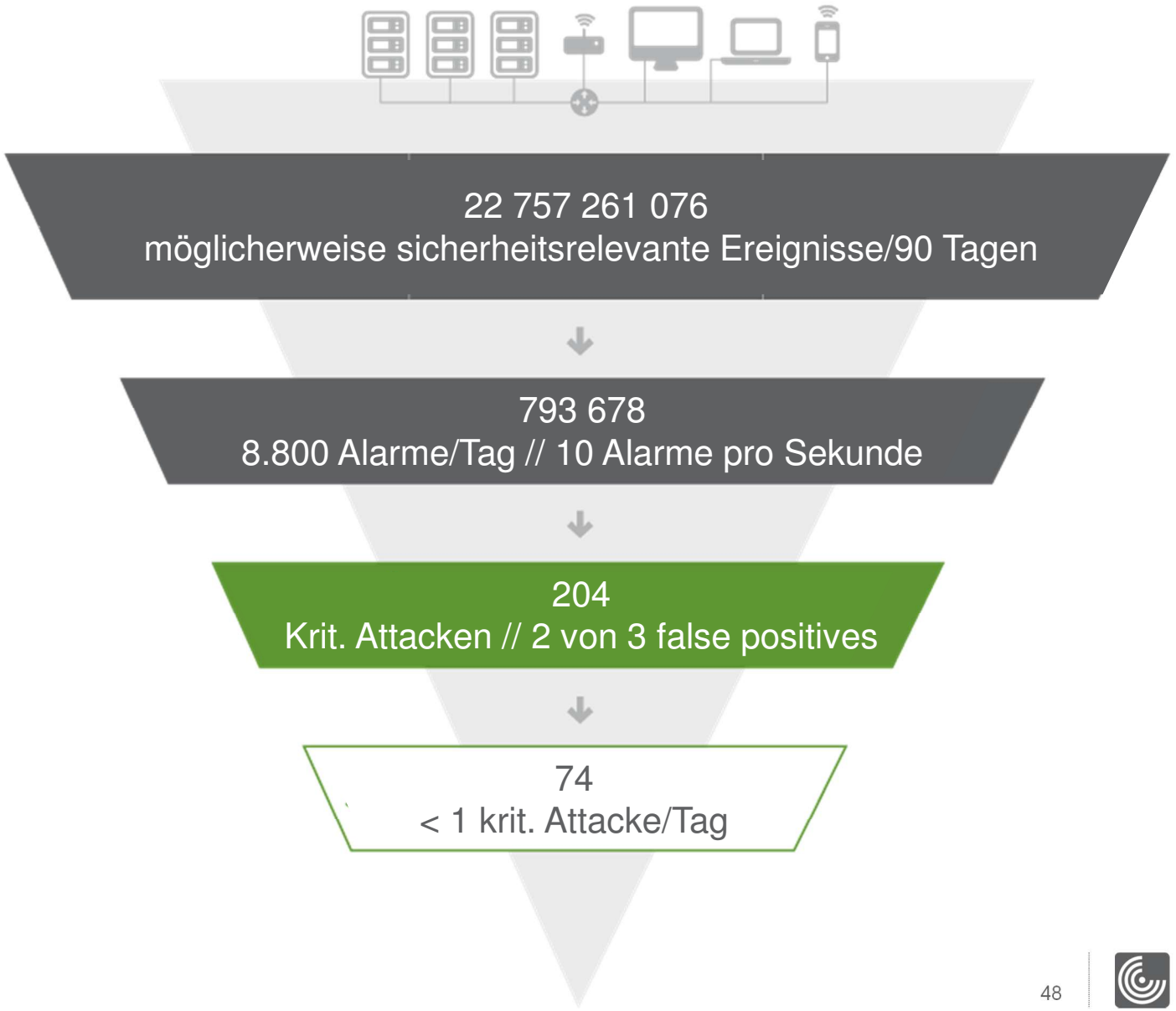
RADAR SERVICES

Next Generation Managed Security Services:



Ihre Daten
verlassen niemals
Ihr Unternehmen.

RADARSERVICES
DAS RESULTAT – Beispiel einer mittelgroßen deutschen Bank



CUSTOMIZED REPORTS & ALARMIERUNG.

- Alarmierung in dringenden Fällen
- Durchgehender Risikobehebungs-Workflow im Cockpit
- Nachrichten-/Feedback-System zur Kommunikation mit dem Intelligence Team
- Integrierter Business Process Risk View zeigt die durch die IT-Sicherheitsprobleme gefährdeten Geschäftsprozesse auf
- Asset Management Funktionen für den Überblick über alle Geräte im Netz

RESULTAT:

ZENTRALE PRÄSENTATION ALLER RISIKO- UND SICHERHEITSINFORMATIONEN

MASSGESCHNEIDERTE, LEICHT VERSTÄNDLICHE BERICHTE & STATISTIKEN IN DER GEWÜNSCHTEN DETAILTIEFE

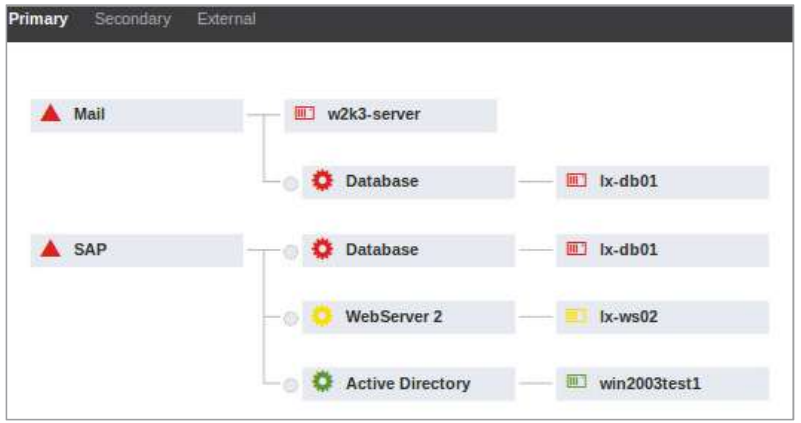
CUSTOMIZED REPORTS IM FOKUS.

RADAR SERVICES

CUSTOMIZED REPORTS
RISIKODARSTELLUNG EN.

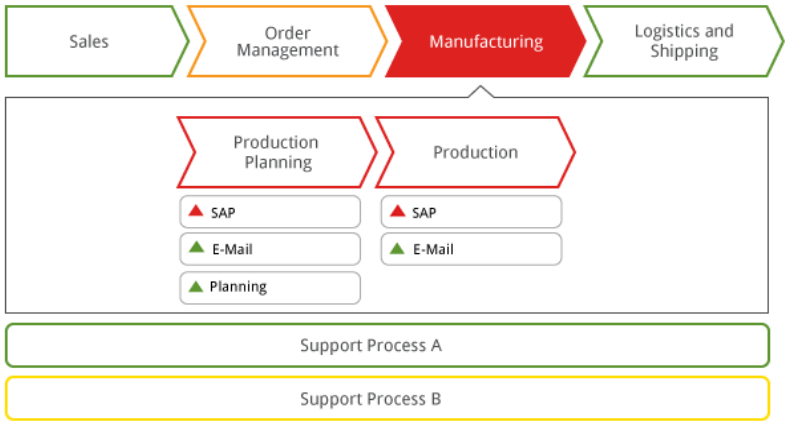
SERVICE VIEW

- Welche IT Services werden benötigt?
- Wie wichtig sind diese?
- Welche Risiken bestehen für die Services?
- Warum sind sie Risiken ausgesetzt?
- Welche Abhängigkeiten bestehen zwischen Services untereinander und zu Assets?

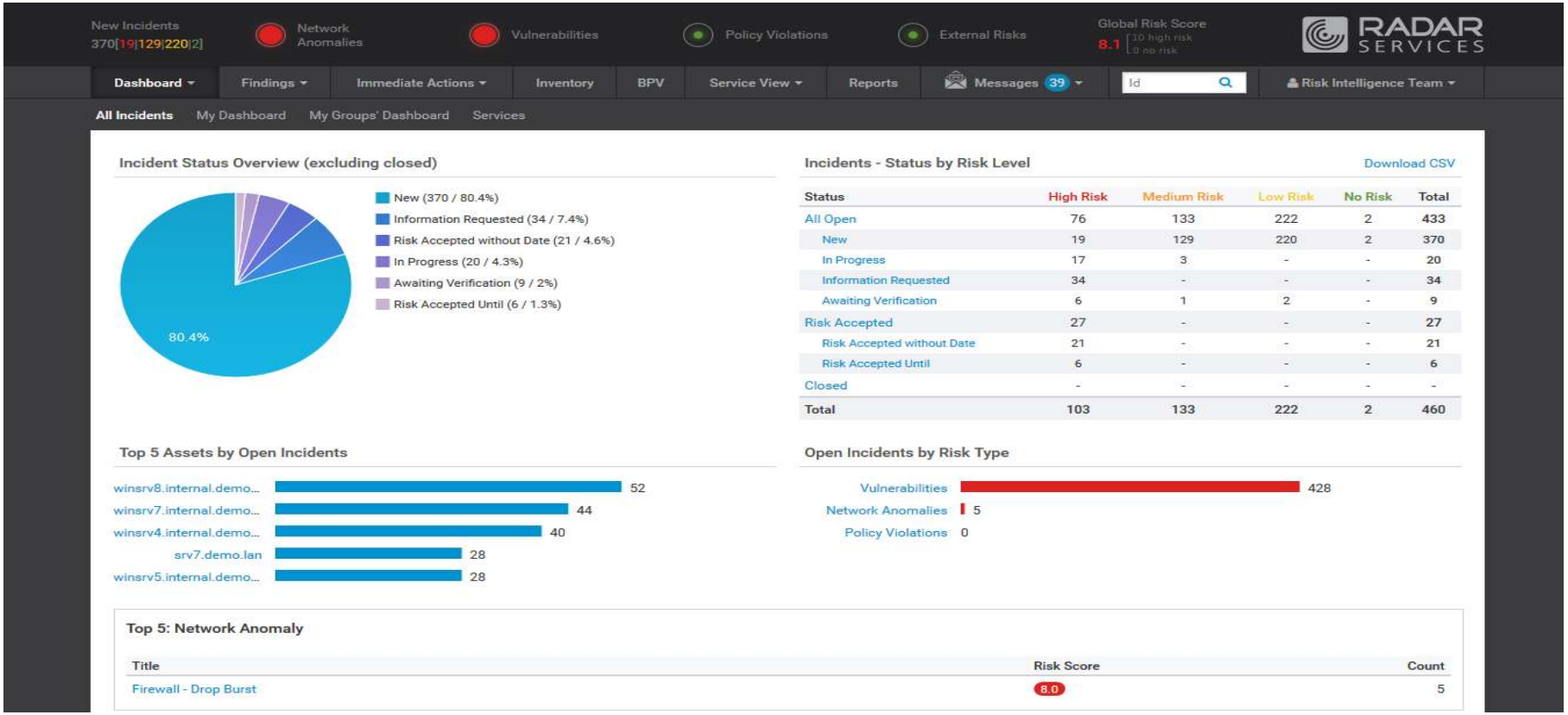


BUSINESS PROCESS VIEW

- Welche Geschäftsprozesse sind durch die Sicherheitsprobleme gefährdet?

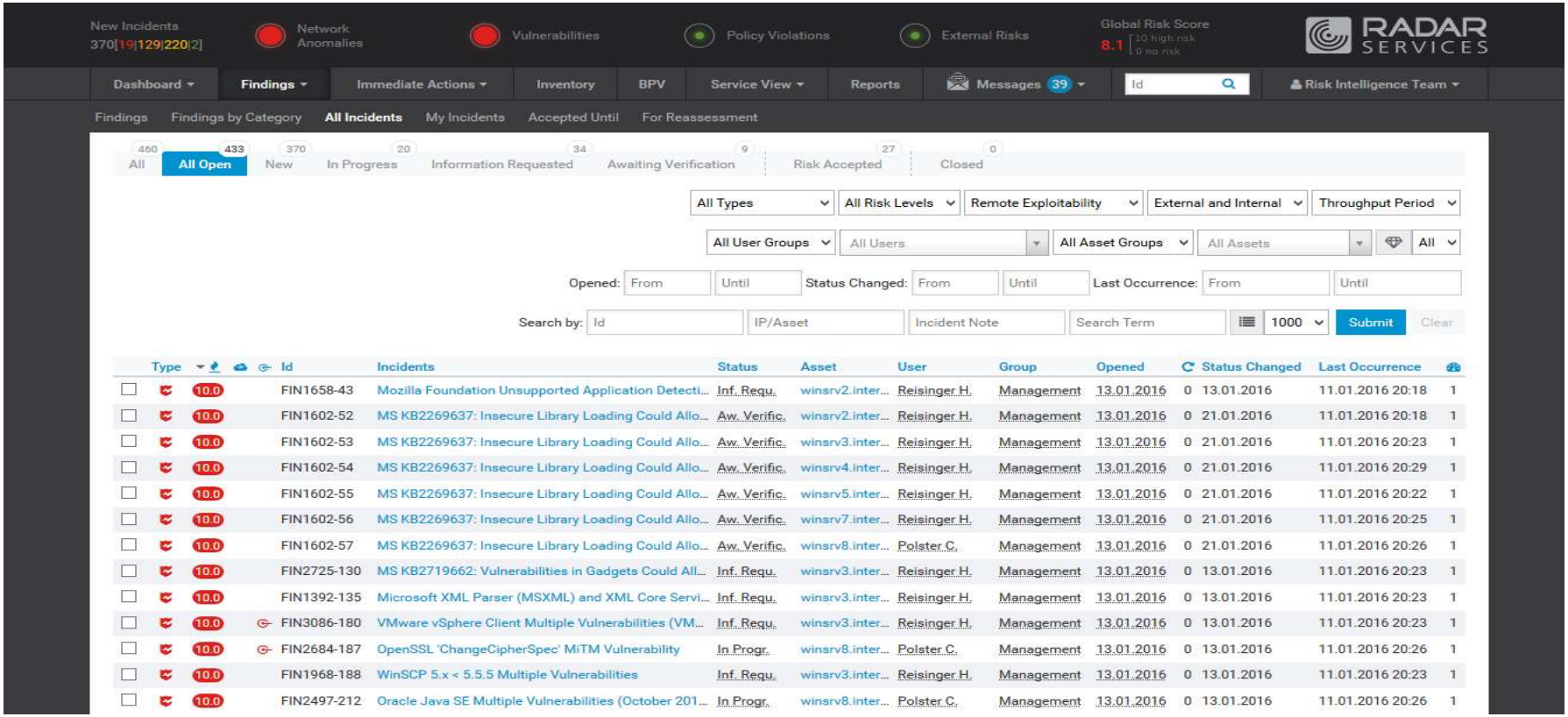


RISK & SECURITY COCKPIT - DASHBOARD



RADAR SERVICES

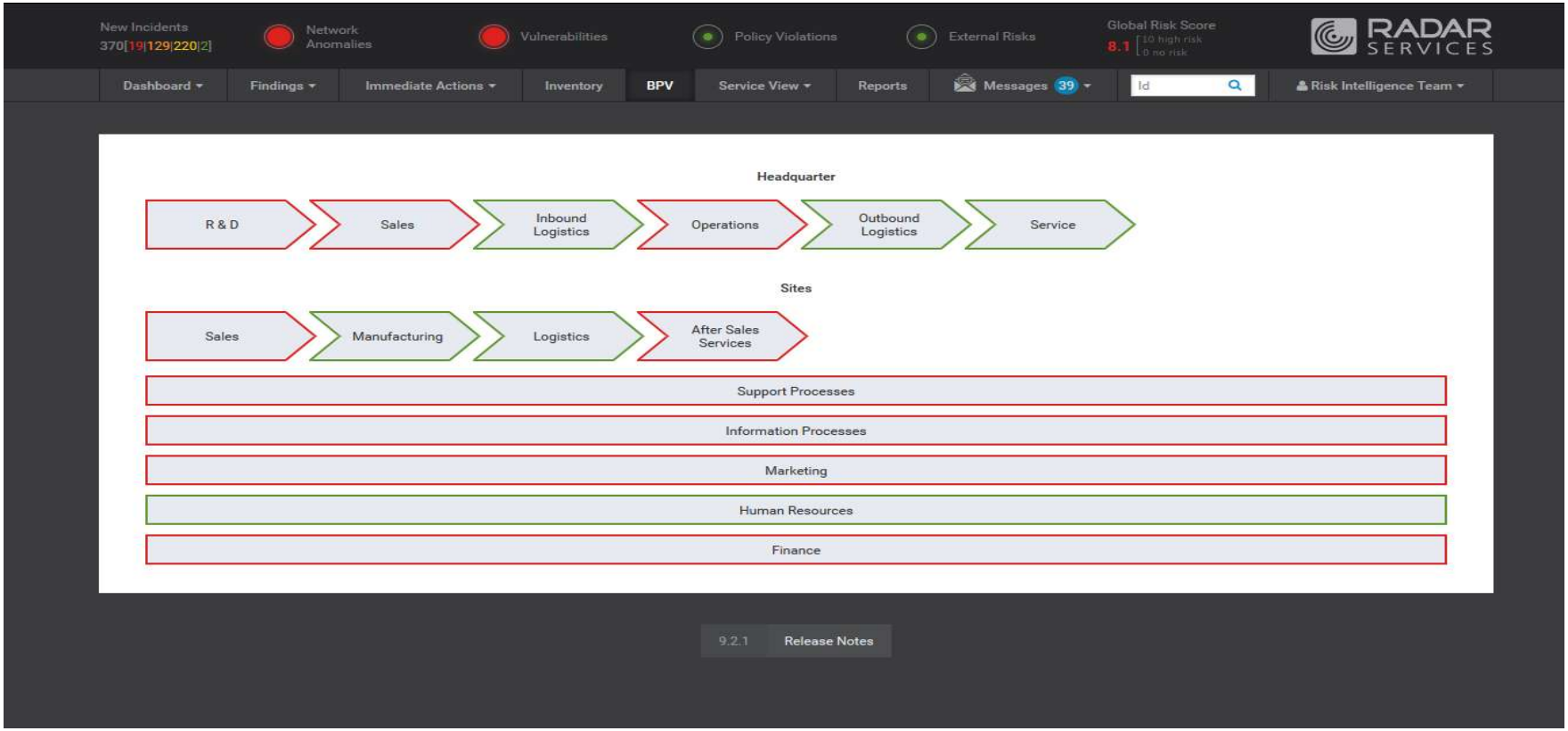
RISK & SECURITY COCKPIT - FINDINGS



Type	Id	Incidents	Status	Asset	User	Group	Opened	Status Changed	Last Occurrence	
10.0	FIN1658-43	Mozilla Foundation Unsupported Application Detecti...	Inf. Requ.	winsrv2.inter...	Reisinger H.	Management	13.01.2016	0 13.01.2016	11.01.2016 20:18	1
10.0	FIN1602-52	MS KB2269637: Insecure Library Loading Could Allo...	Aw. Verific.	winsrv2.inter...	Reisinger H.	Management	13.01.2016	0 21.01.2016	11.01.2016 20:18	1
10.0	FIN1602-53	MS KB2269637: Insecure Library Loading Could Allo...	Aw. Verific.	winsrv3.inter...	Reisinger H.	Management	13.01.2016	0 21.01.2016	11.01.2016 20:23	1
10.0	FIN1602-54	MS KB2269637: Insecure Library Loading Could Allo...	Aw. Verific.	winsrv4.inter...	Reisinger H.	Management	13.01.2016	0 21.01.2016	11.01.2016 20:29	1
10.0	FIN1602-55	MS KB2269637: Insecure Library Loading Could Allo...	Aw. Verific.	winsrv5.inter...	Reisinger H.	Management	13.01.2016	0 21.01.2016	11.01.2016 20:22	1
10.0	FIN1602-56	MS KB2269637: Insecure Library Loading Could Allo...	Aw. Verific.	winsrv7.inter...	Reisinger H.	Management	13.01.2016	0 21.01.2016	11.01.2016 20:25	1
10.0	FIN1602-57	MS KB2269637: Insecure Library Loading Could Allo...	Aw. Verific.	winsrv8.inter...	Polster C.	Management	13.01.2016	0 21.01.2016	11.01.2016 20:26	1
10.0	FIN2725-130	MS KB2719662: Vulnerabilities in Gadgets Could All...	Inf. Requ.	winsrv3.inter...	Reisinger H.	Management	13.01.2016	0 13.01.2016	11.01.2016 20:23	1
10.0	FIN1392-135	Microsoft XML Parser (MSXML) and XML Core Servi...	Inf. Requ.	winsrv3.inter...	Reisinger H.	Management	13.01.2016	0 13.01.2016	11.01.2016 20:23	1
10.0	FIN3086-180	VMware vSphere Client Multiple Vulnerabilities (VM...	Inf. Requ.	winsrv3.inter...	Reisinger H.	Management	13.01.2016	0 13.01.2016	11.01.2016 20:23	1
10.0	FIN2684-187	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	In Progr.	winsrv8.inter...	Polster C.	Management	13.01.2016	0 13.01.2016	11.01.2016 20:26	1
10.0	FIN1968-188	WinSCP 5.x < 5.5.5 Multiple Vulnerabilities	Inf. Requ.	winsrv3.inter...	Reisinger H.	Management	13.01.2016	0 13.01.2016	11.01.2016 20:23	1
10.0	FIN2497-212	Oracle Java SE Multiple Vulnerabilities (October 201...	In Progr.	winsrv8.inter...	Polster C.	Management	13.01.2016	0 13.01.2016	11.01.2016 20:26	1

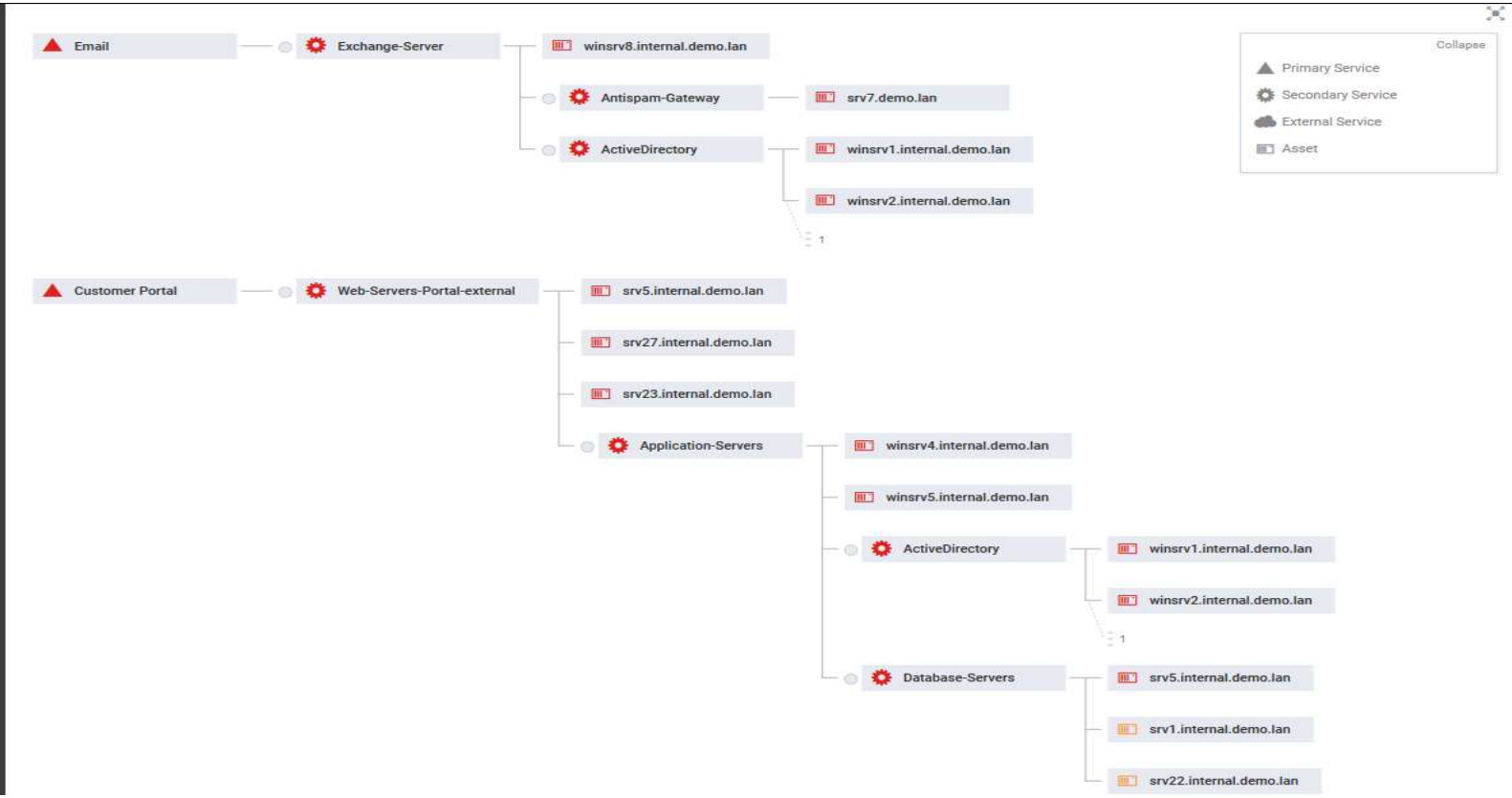
RADAR SERVICES

RISK & SECURITY COCKPIT - BPV



RADAR SERVICES

RISK & SECURITY COCKPIT – SERVICE VIEW



RADAR SERVICES

SICHER, EFFEKTIV & EFFIZIENT.

IHRE DATEN VERLASSEN NIEMALS IHR UNTERNEHMEN.

IHR FRÜHWARN-SYSTEM IST STETS AKTUELL.

IHRE RESSOURCEN WERDEN HÖCHST EFFIZIENT EINGESETZT.

- Speziell gesicherte, im Unternehmensnetzwerk betriebene RadarAppliance beherbergt Module & Advanced Correlation Engine
- Verbindungen zwischen Ihrer Infrastruktur und dem RadarServices SOC mittels sicherer Verbindung mit Mehrfachverschlüsselung (VPN, SSH Tunnel, SSL)
- Laufende Aufzeichnung aller Aktivitäten

SICHER, EFFEKTIV & EFFIZIENT.

IHRE DATEN VERLASSEN NIEMALS IHR UNTERNEHMEN.

IHR FRÜHWARN-SYSTEM IST STETS AKTUELL.

IHRE RESSOURCEN WERDEN HÖCHST EFFIZIENT EINGESETZT.

- Konfiguration und Wartung aller Module durch RadarServices
- Ständige Aktualisierung der Regeln für die Risikoerkennung
- Kontinuierlich erweiterte Regeln und Policies für Advanced Correlation Engine
- Updates für Erkennungsmodule via zentralem Update Service über eine gesicherte Verbindung

SICHER, EFFEKTIV & EFFIZIENT.

IHRE DATEN VERLASSEN NIEMALS IHR UNTERNEHMEN.

IHR FRÜHWARN-SYSTEM IST STETS AKTUELL.

IHRE RESSOURCEN WERDEN HÖCHST EFFIZIENT EINGESETZT.

- Keine zusätzlichen personellen oder finanziellen Ressourcen für Einrichtung, Konfiguration und den täglichen Betrieb
- Kostenersparnisse durch Ablöse von bisher betriebenen Sicherheitslösungen
- Jegliche Kosten für Insellösungen oder zusätzliche Sicherheitslösungen entfallen

Eigenbetrieb eines Security Operation Centers (SOC, Teil eines Cyber Defense Centers) oder als **Managed Service**? - Entscheidungskriterien

DEFINITION SOC.

Ein Security-Operation-Center (SOC) ist eine Kombination aus Experten, Werkzeugen und Prozessen mit dem Ziel, IT Sicherheits-Risiken zu verhindern, zu entdecken, zu analysieren, zu bewerten, deren Behebung zu beschreiben und zu kontrollieren, sowie im Bedarfsfall bei der Umsetzung von Maßnahmen zu unterstützen und Beweissicherung einzuleiten.

EMPFEHLUNGEN FÜR SOC AUFBAU.

- Orientierung am Unternehmensziel (SOC hat keinen eigenen Selbstzweck)
- „A fool with a tool is still a fool“ – Habe oder finde ich das **Fachpersonal** im Unternehmen?
- Paradigmenwechsel berücksichtigen
- SOC Betrieb benötigt Fokus (Ressourcen, Prozesse, mehrere Tools)
- Grundsatzentscheidung: eigenes SOC, Partner finden oder Mischbetrieb
- Strukturierten Aufbau planen:
  - Kein 100% Aufbau in sechs Monaten erreichbar
  - **Personal** finden
  - **Prozesse** planen
  - **Werkzeugportfolio** strukturieren, sukzessive aufbauen **UND** integrieren

DIE WERKZEUGE.
Risikoerkennung und Risikomanagement.

- Schwachstellen-Analyse
- Netzwerk-Risiko-Erkennung (Signatur)
- Netzwerk-Risiko-Erkennung (Verhalten)
- Logdaten-Analyse (SIEM)
- Sandboxing (APT)
- Threat-Intelligence
- Wissensdatenbank (Risiken und Lösungen)
- Workflow-Management-System

INTERN ODER ZUKAUFEN.

Das ist hier die Frage – Beispiel: Mittelständisches Unternehmen 1.000-2.000 Mitarbeiter

» **Interner Aufbau** eines SOC, inkl. Anschaffung der notwendigen Technologien

Beschreibung	Kosten Anschaffung	Kosten jährlich
Technologie	EUR 300.000,00 (HW+Lizenzen)	EUR 60.000,00
Threat Intelligence		EUR 10.000,00
Consulting (extern)		EUR 20.000,00
Personal		EUR 320.000,00 (3 Personen für professionellen SOC Betrieb + 1 Person backup Krankenstand, Urlaub, etc.)
	GESAMT ANSCHAFFUNG	**GESAMT PRO JAHR**
	EUR 300.000,00	**EUR 410.000,00**

» **Managed Service Betrieb** eines SOCs – RadarServices:

- » Setup Kosten (einmalig): 65.000 EUR (Implementierung + anteilig HW)
- » Service Kosten (jährlich): 150.000 EUR

RADAR SERVICES

RADAR SERVICES

Cyber Risiken – Tatsächliche Gefahr für die deutsche Wirtschaft oder nur ein weiterer Hype?

- Definitiv, JA (siehe letzte aktuelle Beispiele in Deutschland der Deutschen Bahn AG, Beiersdorf AG, etc.)

- Cyber Crime und -Terrorismus haben sich zu einem großen Wirtschaftsmarkt mit großer Professionalität entwickelt

- Besonders betroffen sehen wir den deutschen Mittelstand auf Grund teilweiser fehlender Akzeptanz /Budgets, Zuständigkeiten (CISO/CSO, Fachpersonal) und Wissen (Produkt versus Managed Service, fehlende Prozesse und -Personal)

500 Technology Fast 500 2016 EMEA WINNER Deloitte.

IT Security made in Europe

ECS EUROPEAN CYBER SECURITY ORGANISATION

Teilnehmer der Allianz für Cyber-Sicherheit

IT-Security
made in Europe

RADAR SERVICES

VIELEN DANK.

T. +43 (1) 929 12 71-0
sales@radarservices.com
www.radarservices.com

500 | Technology Fast 500 2016 EMEA WINNER Deloitte.

IT Security made in Europe

ECS EUROPEAN CYBER SECURITY ORGANISATION

Teilnehmer der Allianz für Cyber-Sicherheit