Vorstellung pro4bizz GmbH

Ralph Belfiore
Karl Jaeger

Pro4bizz GmbH
https://www.pro4bizz.de
ralph.belfiore@pro4bizz.de
karl.jaeger@pro4bizz.de

0721-909 81 720

Zur pro4bizz GmbH

- Seit vielen Jahren den **Focus** auf **IT Security**, intelligente & integrierbare IT Sicherheits-lösungen, **SIEM**-Strategien, IT-Sicherheitskonzepte
- Seit fast zwei Dekaden Administrations- und Projektunterstützung von **IBM Collaboration Solution Lösungen** (Notes/Domino, Traveler, Sametime, Connections)
- Zertifizierte **Systemadministratoren** und **Trainer** für **Notes** und **Domino**, durchgängig seit Lotus Notes Version 4, aktuell Version 9.0
- Zertifizierte Trainer für **IBM QRadar**
- Zertifizierte IT-Security-Beauftrage für EVU
- Seit einigen Jahren beschäftigen wir uns mit dem Thema „**My mobile Workplace**". Dabei verfolgen wir die Strategie „Security First – Mobile always“ und verknüpfen aktuelle Soft- und Hardwaretechnologien
  - **Security Intelligence**
  - Desktop **Virtualisierung**, Thin-Client Strategien(**Vmware View**)
  - Aufbau und Organisation von ISMS
  - Konzeption und Aufbau von SIEM Infrastrukturen auf Basis ISO 27001

Warum brauchen wir heute intelligente IT-Sicherheits-Lösungen?

Wissen Sie was gerade JETZT in Ihrer IT Infrastruktur passiert?

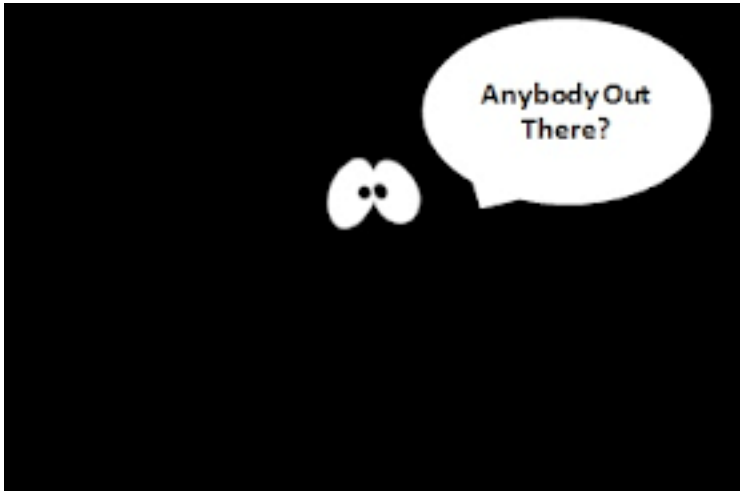
Sicherheitsvorfälle rechtzeitig erkennen!

Unsere moderne Gesellschaft

Heute sind wir in hohem Maße von einer funktionierenden IT-Intrastruktur abhängig.

Unsere moderne Gesellschaft

Fehlen z. B. Benzin, Gas, Geld, Lebensmittel, Strom, Transport, Wass oder auch jede Form von Telekommunikation kommt das öffentliche Leben innerhalb kürzester Zeit zum Erliegen und lebensnotwendige Dienstleistungen können nicht mehr erbracht werden.



Intakte Informations- und Kommunikationstechnologie

Gleichzeitig ist die Funktionsfähigkeit der Energieversorgung von einer intakten IKT abhängig.

Schutz gegen Bedrohungen

Um die Vorteile moderner IKT auch in Zukunft sicher nutzen zu können, ist es wichtig, einen angemessenen Schutz gegen Bedrohungen für IKT-Systeme zu etablieren.

IT Sig/IT SiKat

25.7.2015: IT-Sicherheitsgesetz – Inkrafttreten des IT-SIG

Ziel: **Deutschland will die sichersten IT-Systeme & digitalen Infrastrukturen weltweit**

IT Sig/IT SiKat

12.8.2015: Veröffentlichung des IT-SiKat
Gemäß §11 Absatz 1a Energiewirtschaftsgesetz (EnWG)

Geltungsbereich:
Alle zentralen und dezentralen Anwendungen, Systeme und Komponenten die der Netzsteuerung und –überwachung dienen und zur Gewährleistung des stabilen und sicheren Netzbetriebs benötigt werden.

IT Sig/IT SiKat

Kernanforderung:

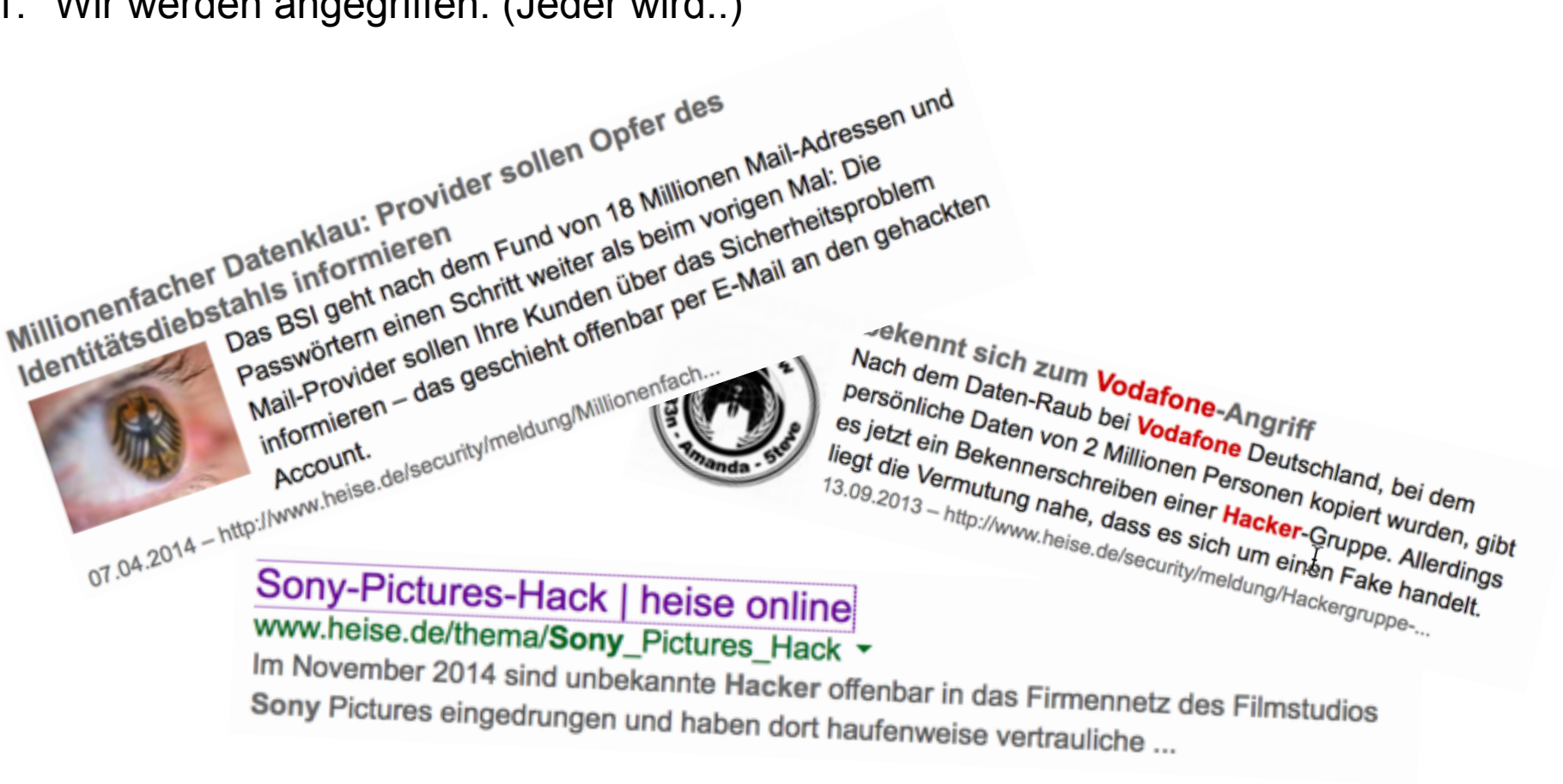
- **Einführung eines ISMS gemäß ISO27001**, Umsetzungsfrist bis 31.1.2018, Zertifizierung durch unabhängige Stelle und
- Benennung eines Ansprechpartners IT-Sicherheit für die Bundesnetzagentur – Umsetzung war 30.11.2015

Warum brauchen wir heute intelligente IT-Sicherheits-Lösungen?

IT-Sicherheit 1.0 – Es ist Zeit für einen Strategiewechsel!

Warum brauchen wir heute intelligente IT-Sicherheits-Lösungen?

1. Wir werden angegriffen. (Jeder wird..)



Warum brauchen wir heute intelligente IT-Sicherheits-Lösungen?

1. Wir werden angegriffen. (Jeder wird..)

MySpace
Hacker knacken MySpace und erbeuten Millionen von Zugangsdaten

Montag, 30.05.2016, 15:45

US-Medienberichten zufolge ist das soziale Netzwerk MySpace offenbar von einem massiven Hacker-Angriff betroffen. Es wurden rund 427 Millionen Passwörter erbeutet und 360 Millionen E-Mail-Adressen. Nutzer sind angehalten, ihr Passwort zu ändern.

Nach LinkedIn hat es nun auch MySpace erwischt

oppi / Shutterstock.com

Facebook, **Instagram**, **Snapchat** und Co. kennt jeder. Doch kann sich noch jemand an MySpace erinnern? Zugegeben: Das soziale Netzwerk hat massiv an Bedeutung verloren. Dennoch sollten Nutzer sicherheitshalber ihr Passwort ändern, denn ein Hacker hat offenbar Millionen von Zugangsdaten erbeutet.

www.focus.de

Sicherheit

117 Mio. Passwörter aus LinkedIn-Hack: Warum Kommunikation nach einem Hack das A und O ist

26. Mai 2016 • 2 Kommentare

www.basicthinking.de

iX 12/2016, Seite 88

Sicherheit – Report

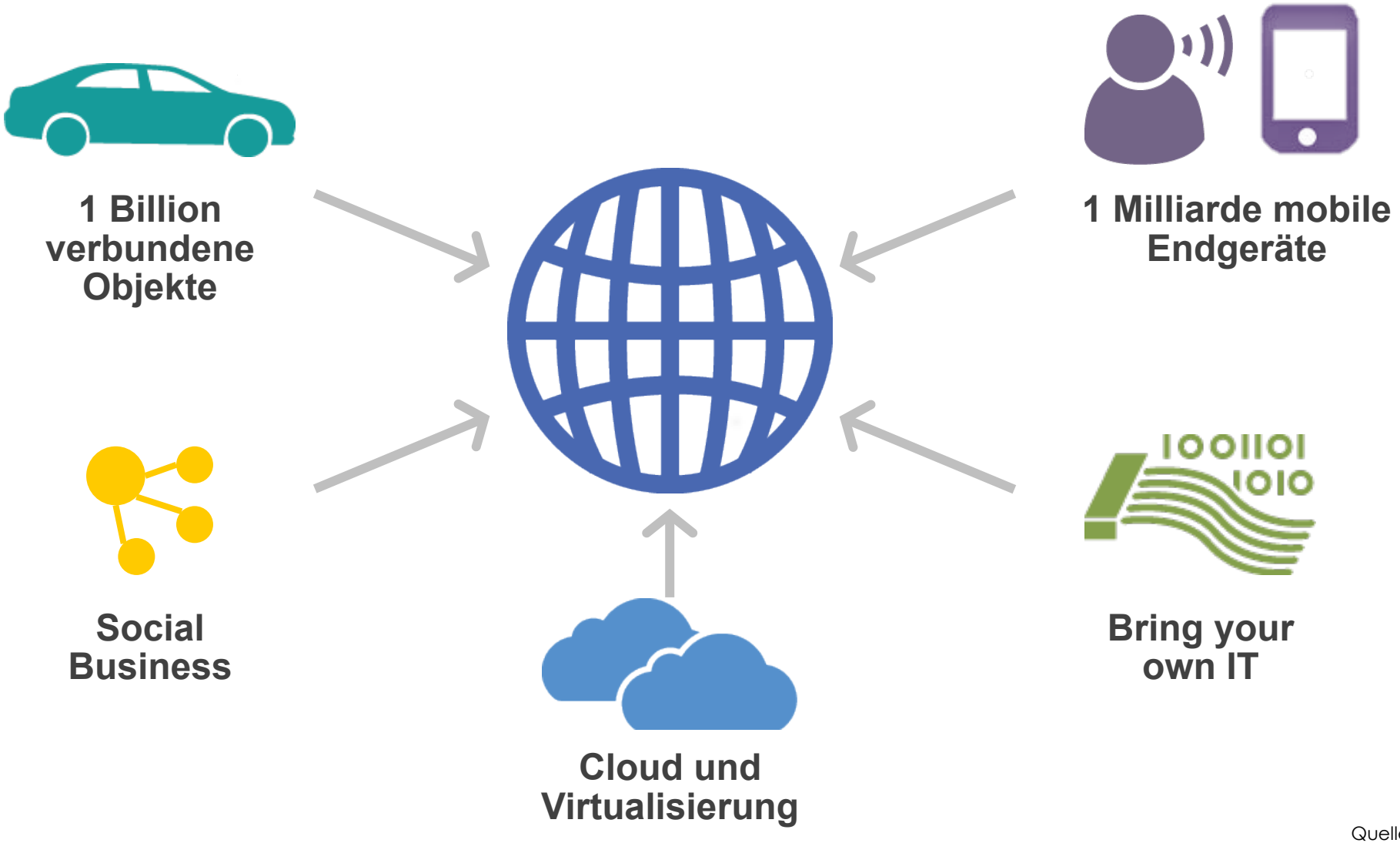
Digitales Bombardement

Das Internet der Dinge verstärkt DDoS-Angriffe

Im Herbst 2016 fanden die bisher heftigsten verteilten Angriffe auf den unverzichtbaren Internetdienst DNS statt. Noch größeres Unheil steht zu befürchten, doch Anwender und Anbieter sind nicht vollkommen wehrlos.

www.ix.de/ix1612088

Innovative Technologien/IOT verändern alles!



Quelle: IBM

Die Motivation für Angriffe ist vielfältig

Nationale Sicherheit

Staatliche Akteure
Stuxnet

Spionage, Aktivismus

Wettbewerber und Hacktivisten
Aurora

Monetärer Nutzen

Organisiertes Verbrechen
Zeus

Rache, Neugierde

Insider und Script-kiddies
"I love you"

Quelle: IBM

Zunehmende Anzahl von Sicherheitsbedrohungen

Nahezu tägliche Lecks sensitiver Daten

40% Anstieg

gemeldete Datenpannen und Ereignissen

Schonungslose Verwendung unzähliger Methoden

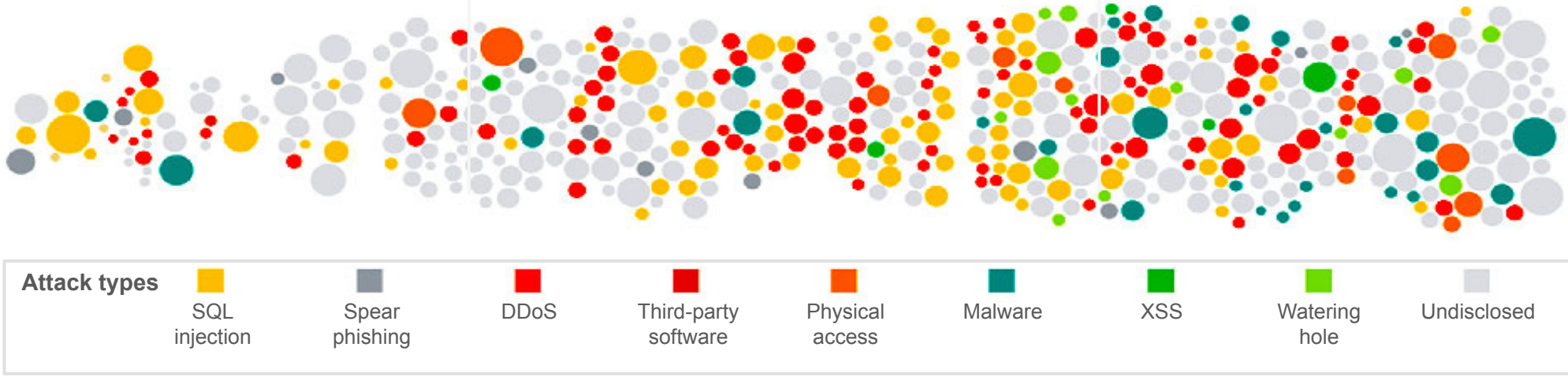
800,000,000+ Aufzeichnungen

.., während die Zukunft keine Anzeichen der Änderung zeigt

"verrückt" Gemeldete Anzahl an Vorfällen

42% der CISOs

Beklagen dass das Risiko externer Bedrohungen sich von Jahr zu Jahr dramatisch erhöht



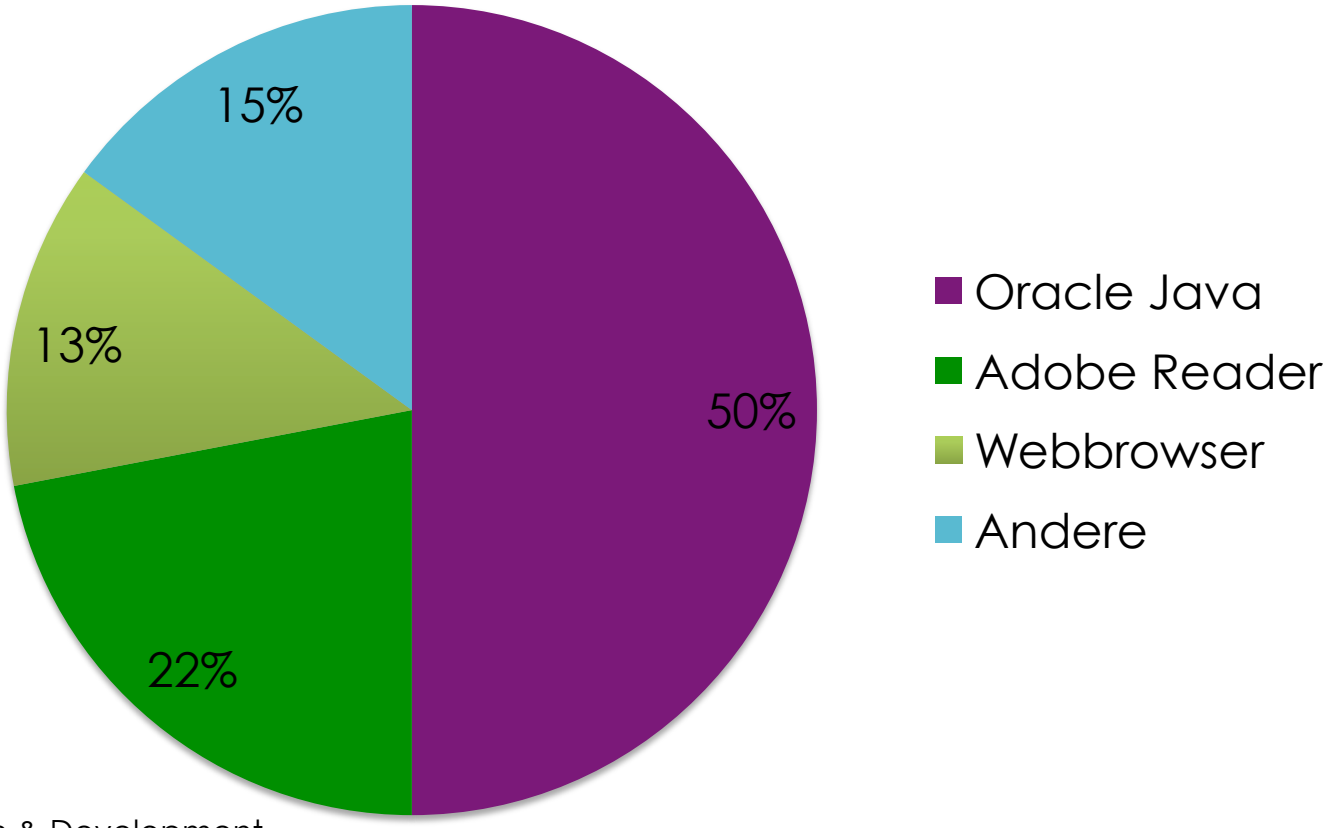
Note: Size of circle estimates relative impact of incident in terms of cost to business.

Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015

Quelle: IBM

Was sehen wir heute?

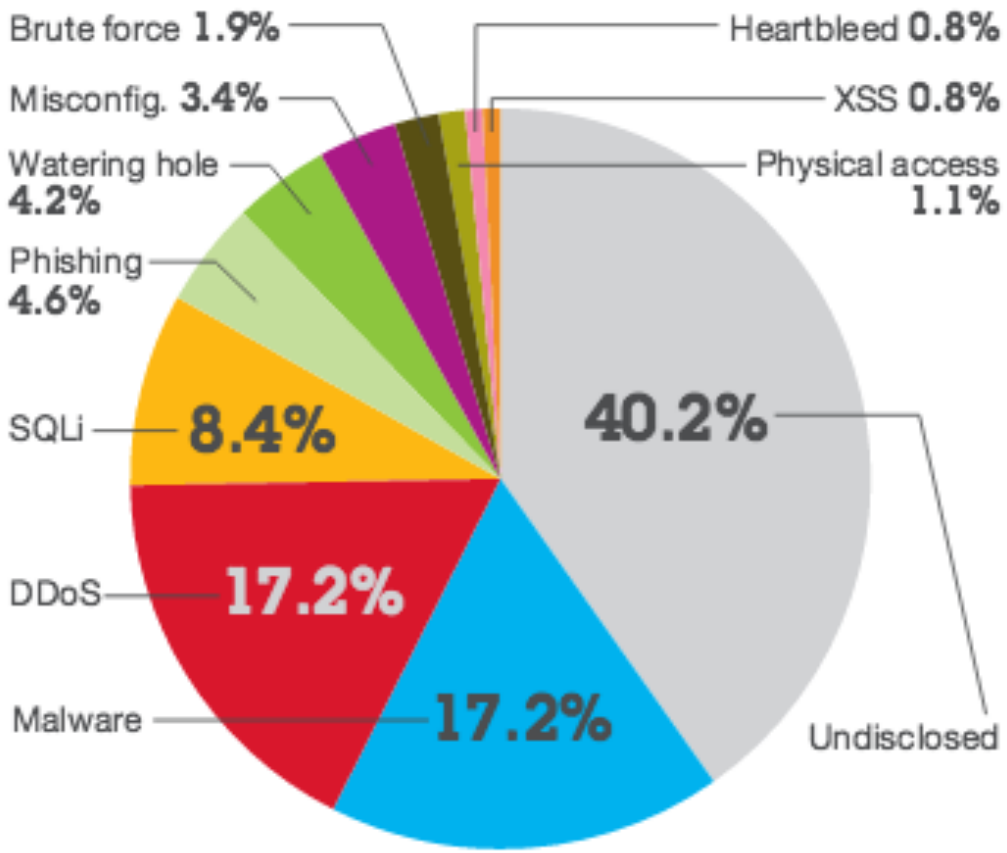
- Angriffe auf Anwendungen



Quelle: IBM X-Force Research & Development

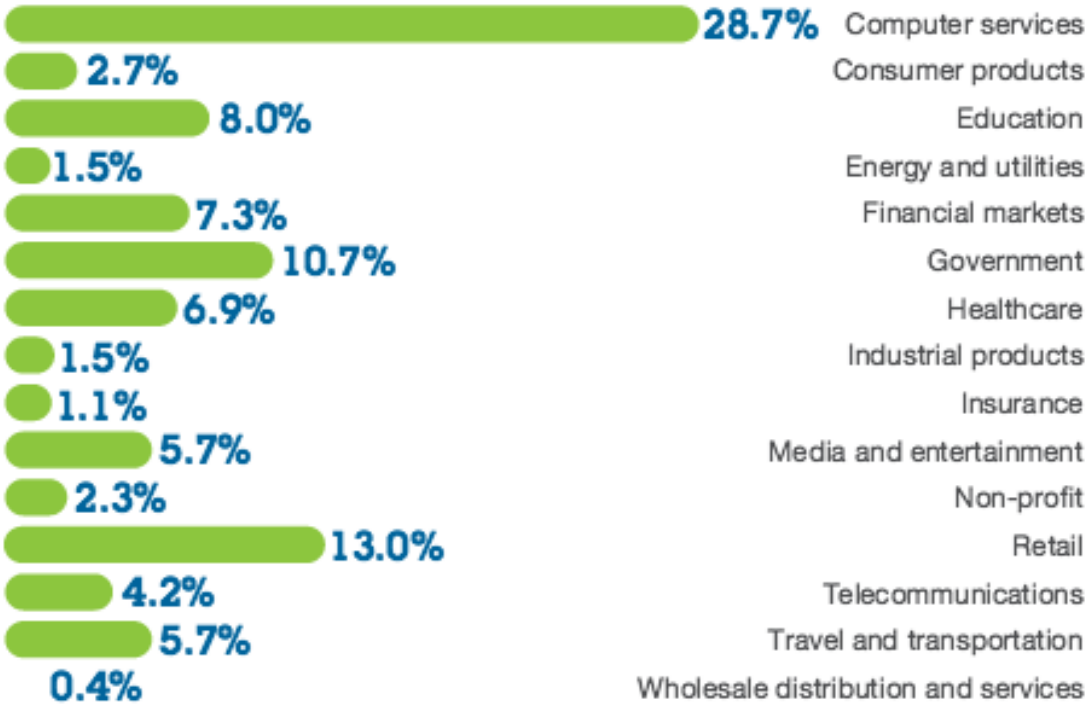
Was sehen wir heute?

- Die am häufigsten gebrauchten Angriffstypen



Quelle: IBM X-Force Research & Development

Welche Branchen werden wie angegriffen?



Advanced Persistent Thread ist die verbreiteste Methode der professionellen Hacker

Quelle: IBM X-Force Research & Development

Was ist ein "Advanced Persistent Threat?"

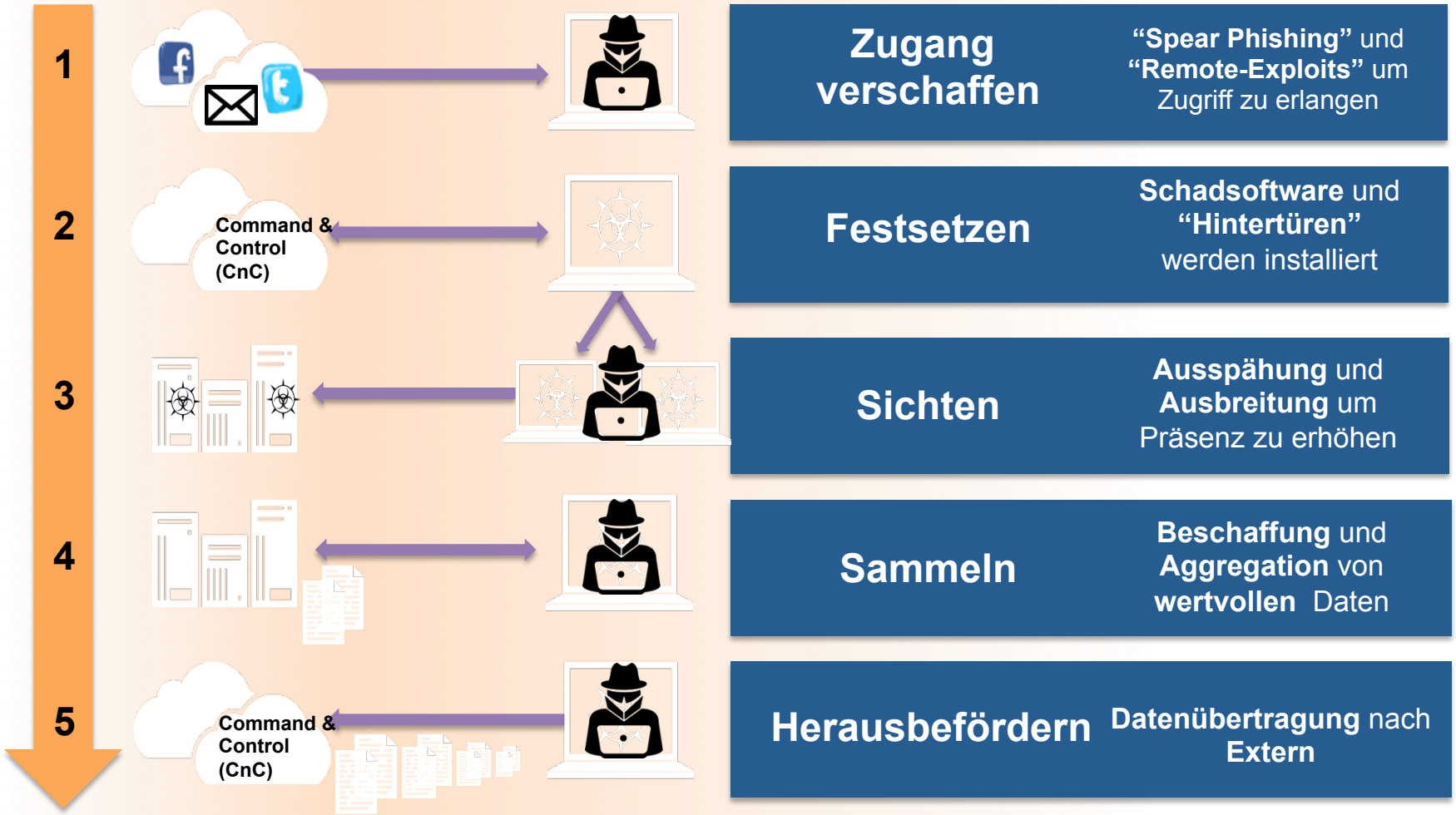
1. Nutzt unbekannte („**Zero Day**") Schwachstellen aus

2. Angriffe dauern **Monate** oder **Jahre**
(durchschnittlich 1 Jahr, höchstens 4.8 Jahre)

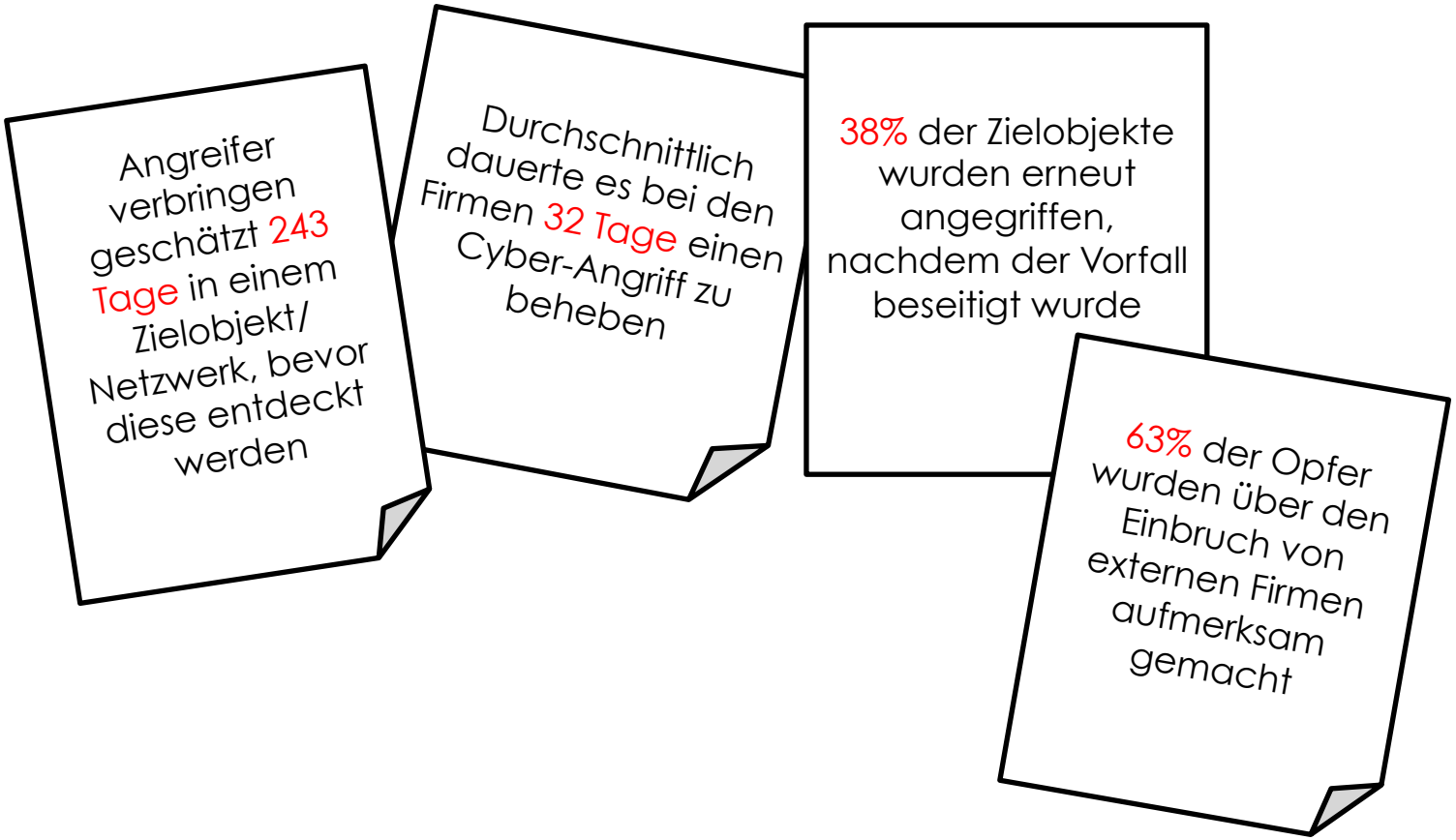
3. Visiert **spezielle Personen** oder **Gruppen einer Organisation** an

Quelle: IBM

Cyber-Angriff: Angreifer folgen 5-Phasen während eines Angriffs



Eine klare und eindeutige Bedrohungslage



Quelle: IBM

Security Incident – Workflow – Gezielte Maßnahmen durchführen

1. Was passiert gerade in Ihrem Netzwerk?
   - Ist Ihnen das vollumfänglich bekannt?

2. Wenn Sie angegriffen werden, wie schnell können Sie aktuell reagieren? Zeit ist ein wesentlicher Faktor!
   - Und sind Sie gründlich genug beim Aufräumen?

Das Schadsoftware ins Haus kommt, lässt sich nicht verhindern

E-Mail Trojaner: Ikea-Mails enthalten **Schadsoftware**

T-Online - vor 4 Tagen

Der E-Mail-Anhang spricht aber eindeutig für Online-Kriminelle. Wer die angehängte Datei ausführt, lädt sich eine **Schadsoftware** auf den ...

Gartner Quadrant – Hersteller im Bereich Security

Sensibilität und Sensorik, um Cyber-Angriffe zu erkennen

19.06.2013 15:45

« Vorige | Nächste »

Merkel: "Das Internet ist für uns alle Neuland"

"Das Internet ist für uns alle Neuland", sagte die Kanzlerin. Nötig sei eine Balance, um den Menschen gleichzeitig Sicherheit zu bieten, ihnen aber nicht ihre Unbeschwertheit beim Umgang mit den neuen Medien zu nehmen.

Es muss nicht immer der Hacker sein – Sicherheitslücken sind oft hausgemacht

- Unvollständige Dokumentation
- Ungenehmigte technische Maßnahmen
- Korrupte Datensätze
- Social Engineering
- Fehlende Prozesse für Alltag & Notfall
- Unkontrollierter Datenaustausch
- Priorisierung & Überlastung

Faktor Mensch = Risiko & Erfolg

Awareness der Anwender

- Warum öffnen Anwender unbekannte Links?

Klassische Verwaltung von PC Arbeitsplätzen kommt an Grenzen

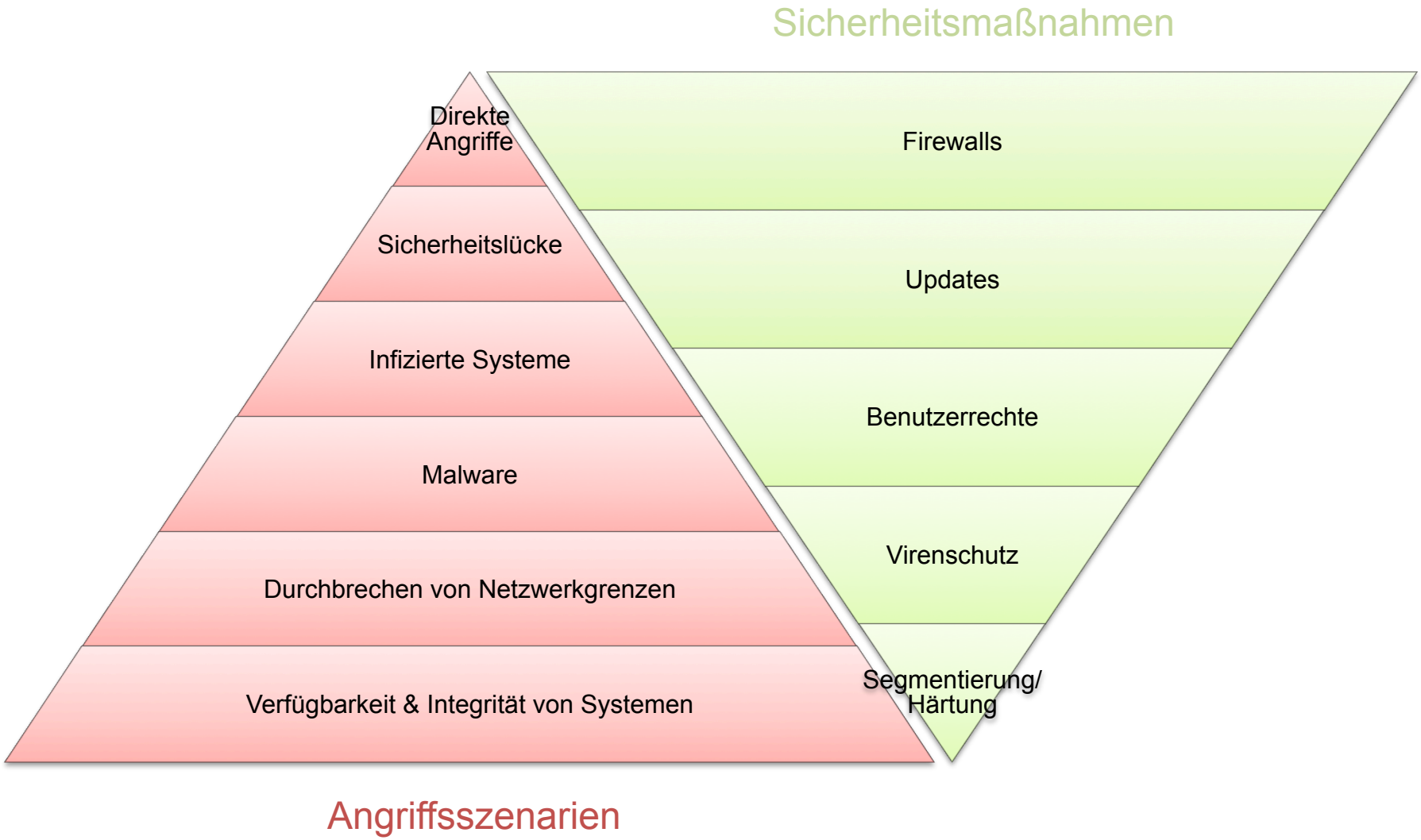
Updates

Security-Patches

Schwachstellen

Natürlich hat jeder bereits Sicherheitsmaßnahmen – Aber:

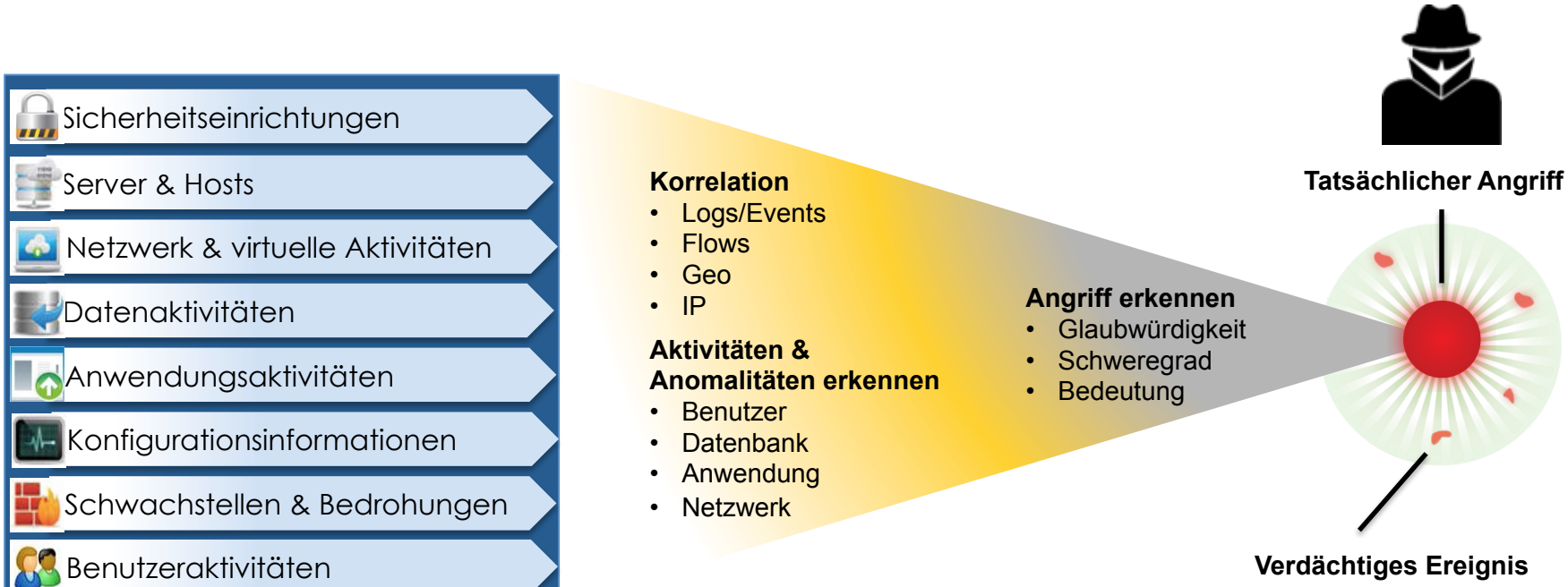
Wir müssen die richtigen Dinge tun – und die Dinge richtig tun!



IT Sicherheitsmaßnahmen

Ohne ein strategisches Gesamtkonzept stehen die meisten IT-Sicherheitsmaßnahmen „alleine“ da

Security Intelligence Plattform: Echtzeitkorrelation entdeckt priorisierte Vorfälle

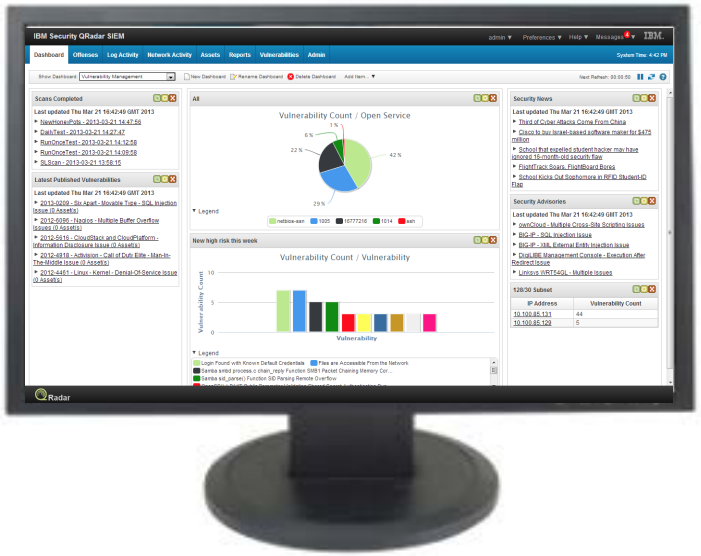


Umfassende Datenquellen + Tiefgehende Erkenntnis = Besonders sorgfältige und belangbare Einblicke

Quelle: IBM

Im Mittelpunkt: Früherkennung von Anomalitäten!

Personen
schützen und beobachten von Zugriffen auf IT- Systeme, Informationen und Anwendungen



Untersuchung
ständige Beobachtung der Bedrohungslandschaft durch neue Schwachstellen

Daten
ständiges beobachten und bewerten von Datenbanken, Dateiverzeichnissen und Big-Data Umgebungen

Anwendungen
erkennen und beseitigen von Schwachstellen in Webanwendungen, bevor sie betroffen sind

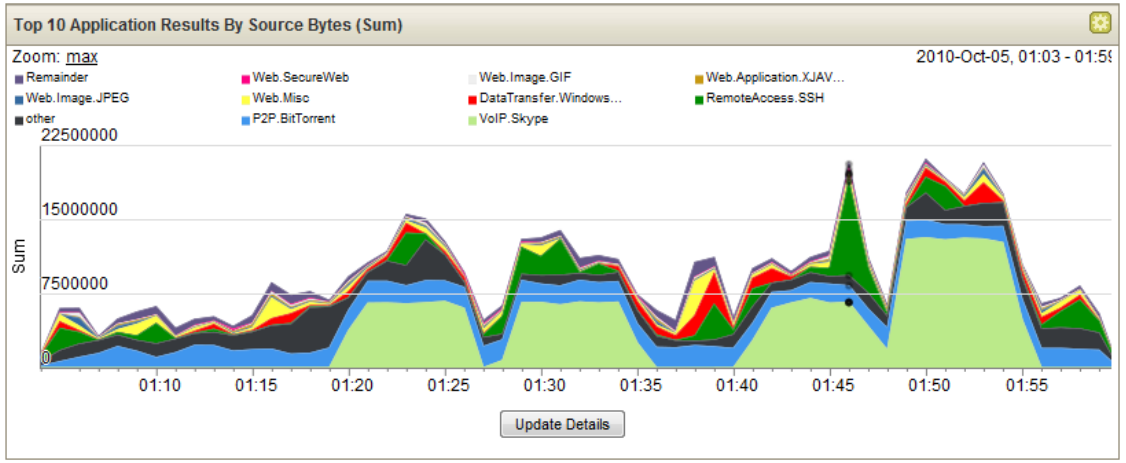
Infrastruktur
erkennen, beseitigen und blocken von Bedrohungen durch ständig wechselnde Server, Netzwerke und Endpunkte

Quelle: IBM

Transparenz: Netzwerk Flow-Analyse

- Netflows ermöglichen einen Einblick in die Angreifer-Kommunikation
- Einblick in Layer 7 Anwendungsinformationen erhöhen Transparenz
- Portbasierte Firewalls kommen an Grenzen

Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101
VoIP.Skype	Multiple (5)						9 290
RemoteAccess.SSH	Multiple (10)						3 020
Web.Misc	Multiple (16)						5 741
Web.Application.Misc	Multiple (9)						5 267

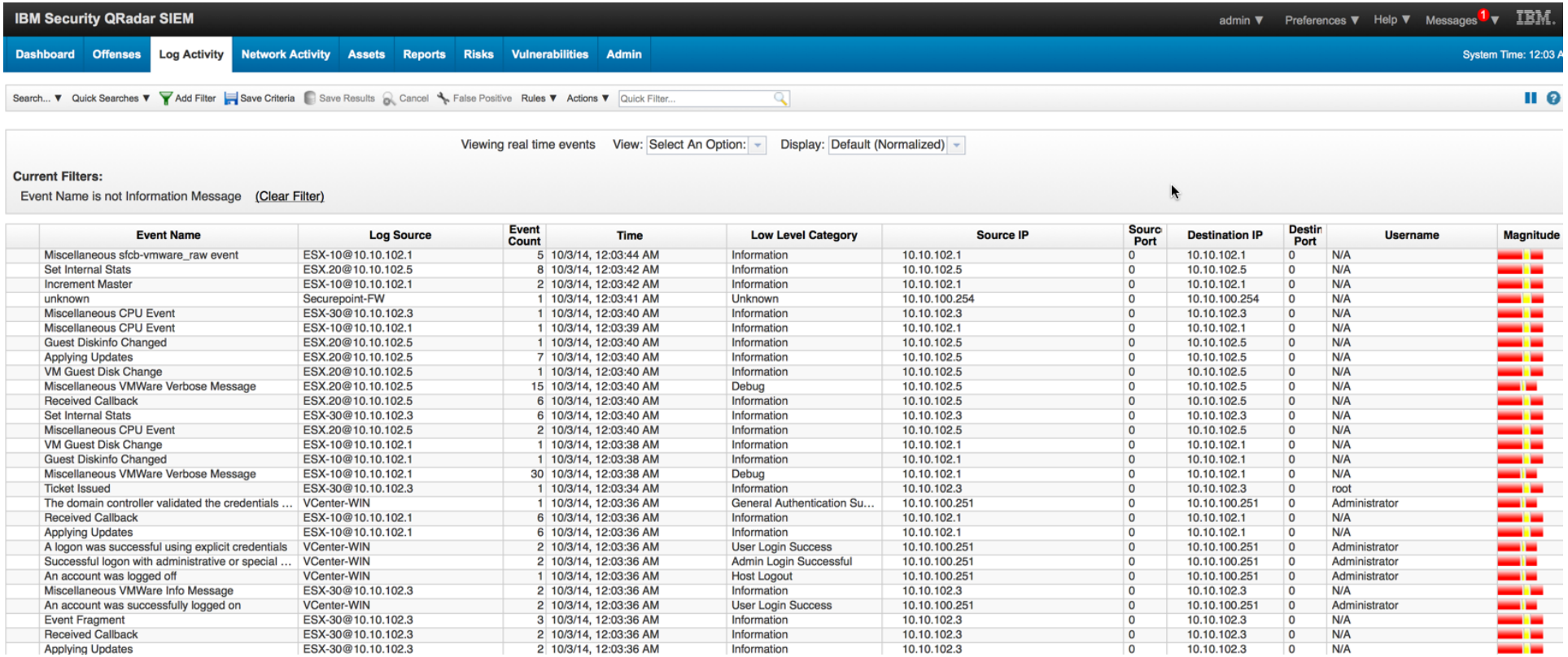


Transparenz: Netzwerk Flow-Analyse

- Netflows ermöglichen einen Einblick in die Angreifer-Kommunikation
- Einblick in Layer 7 Anwendungsinformationen erhöhen Transparenz
- Egal welche Anwendung…

Transparenz: Logaktivitäten der relevanten IT Komponenten

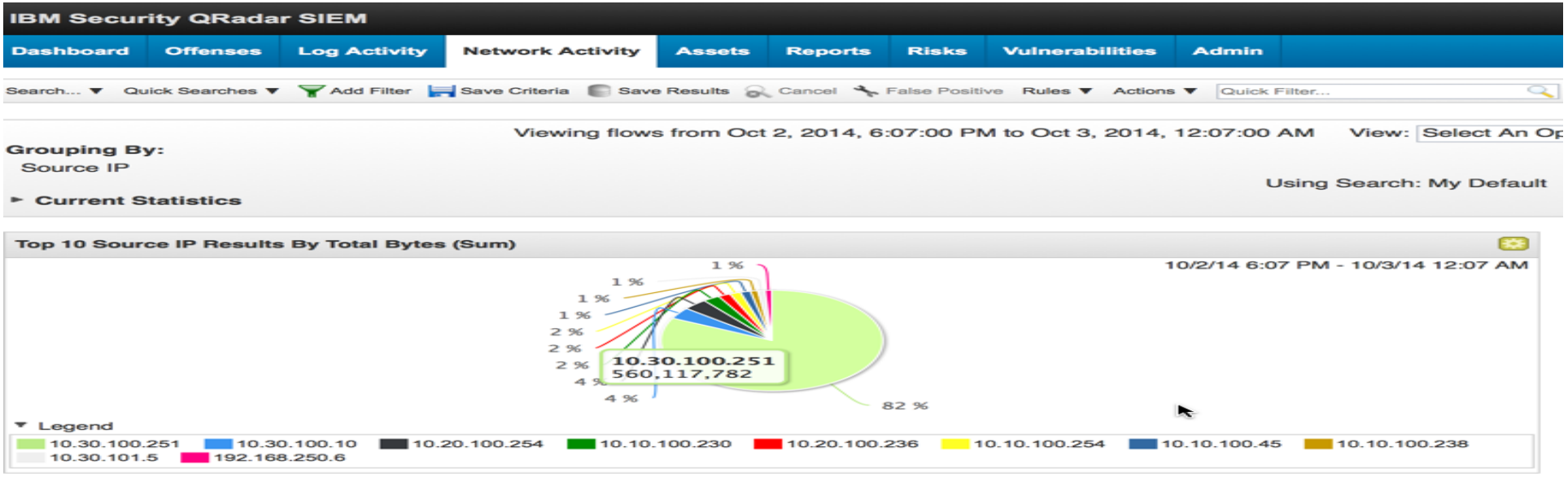
- Korrelieren von Log-/Eventinformationen relevanter Systeme



Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Miscellaneous sfcb-vmware_raw event	ESX-10@10.10.102.1	5	10/3/14, 12:03:44 AM	Information	10.10.102.1	0	10.10.102.1	0	N/A	
Set Internal Stats	ESX.20@10.10.102.5	8	10/3/14, 12:03:42 AM	Information	10.10.102.5	0	10.10.102.5	0	N/A	
Increment Master	ESX-10@10.10.102.1	2	10/3/14, 12:03:42 AM	Information	10.10.102.1	0	10.10.102.1	0	N/A	
unknown	Securepoint-FW	1	10/3/14, 12:03:41 AM	Unknown	10.10.100.254	0	10.10.100.254	0	N/A	
Miscellaneous CPU Event	ESX-30@10.10.102.3	1	10/3/14, 12:03:40 AM	Information	10.10.102.3	0	10.10.102.3	0	N/A	
Miscellaneous CPU Event	ESX-10@10.10.102.1	1	10/3/14, 12:03:39 AM	Information	10.10.102.1	0	10.10.102.1	0	N/A	
Guest Diskinfo Changed	ESX.20@10.10.102.5	1	10/3/14, 12:03:40 AM	Information	10.10.102.5	0	10.10.102.5	0	N/A	
Applying Updates	ESX.20@10.10.102.5	7	10/3/14, 12:03:40 AM	Information	10.10.102.5	0	10.10.102.5	0	N/A	
VM Guest Disk Change	ESX.20@10.10.102.5	1	10/3/14, 12:03:40 AM	Information	10.10.102.5	0	10.10.102.5	0	N/A	
Miscellaneous VMWare Verbose Message	ESX.20@10.10.102.5	15	10/3/14, 12:03:40 AM	Debug	10.10.102.5	0	10.10.102.5	0	N/A	
Received Callback	ESX.20@10.10.102.5	6	10/3/14, 12:03:40 AM	Information	10.10.102.5	0	10.10.102.5	0	N/A	
Set Internal Stats	ESX-30@10.10.102.3	6	10/3/14, 12:03:40 AM	Information	10.10.102.3	0	10.10.102.3	0	N/A	
Miscellaneous CPU Event	ESX.20@10.10.102.5	2	10/3/14, 12:03:40 AM	Information	10.10.102.5	0	10.10.102.5	0	N/A	
VM Guest Disk Change	ESX-10@10.10.102.1	1	10/3/14, 12:03:38 AM	Information	10.10.102.1	0	10.10.102.1	0	N/A	
Guest Diskinfo Changed	ESX-10@10.10.102.1	1	10/3/14, 12:03:38 AM	Information	10.10.102.1	0	10.10.102.1	0	N/A	
Miscellaneous VMWare Verbose Message	ESX-10@10.10.102.1	30	10/3/14, 12:03:38 AM	Debug	10.10.102.1	0	10.10.102.1	0	N/A	
Ticket Issued	ESX-30@10.10.102.3	1	10/3/14, 12:03:34 AM	Information	10.10.102.3	0	10.10.102.3	0	root	
The domain controller validated the credentials ...	VCenter-WIN	1	10/3/14, 12:03:36 AM	General Authentication Su...	10.10.100.251	0	10.10.100.251	0	Administrator	
Received Callback	ESX-10@10.10.102.1	6	10/3/14, 12:03:36 AM	Information	10.10.102.1	0	10.10.102.1	0	N/A	
Applying Updates	ESX-10@10.10.102.1	6	10/3/14, 12:03:36 AM	Information	10.10.102.1	0	10.10.102.1	0	N/A	
A logon was successful using explicit credentials	VCenter-WIN	2	10/3/14, 12:03:36 AM	User Login Success	10.10.100.251	0	10.10.100.251	0	Administrator	
Successful logon with administrative or special ...	VCenter-WIN	2	10/3/14, 12:03:36 AM	Admin Login Successful	10.10.100.251	0	10.10.100.251	0	Administrator	
An account was logged off	VCenter-WIN	1	10/3/14, 12:03:36 AM	Host Logout	10.10.100.251	0	10.10.100.251	0	Administrator	
Miscellaneous VMWare Info Message	ESX-30@10.10.102.3	2	10/3/14, 12:03:36 AM	Information	10.10.102.3	0	10.10.102.3	0	N/A	
An account was successfully logged on	VCenter-WIN	2	10/3/14, 12:03:36 AM	User Login Success	10.10.100.251	0	10.10.100.251	0	Administrator	
Event Fragment	ESX-30@10.10.102.3	3	10/3/14, 12:03:36 AM	Information	10.10.102.3	0	10.10.102.3	0	N/A	
Received Callback	ESX-30@10.10.102.3	2	10/3/14, 12:03:36 AM	Information	10.10.102.3	0	10.10.102.3	0	N/A	
Applying Updates	ESX-30@10.10.102.3	2	10/3/14, 12:03:36 AM	Information	10.10.102.3	0	10.10.102.3	0	N/A	

Transparenz: Netzwerkaktivitäten erkennen

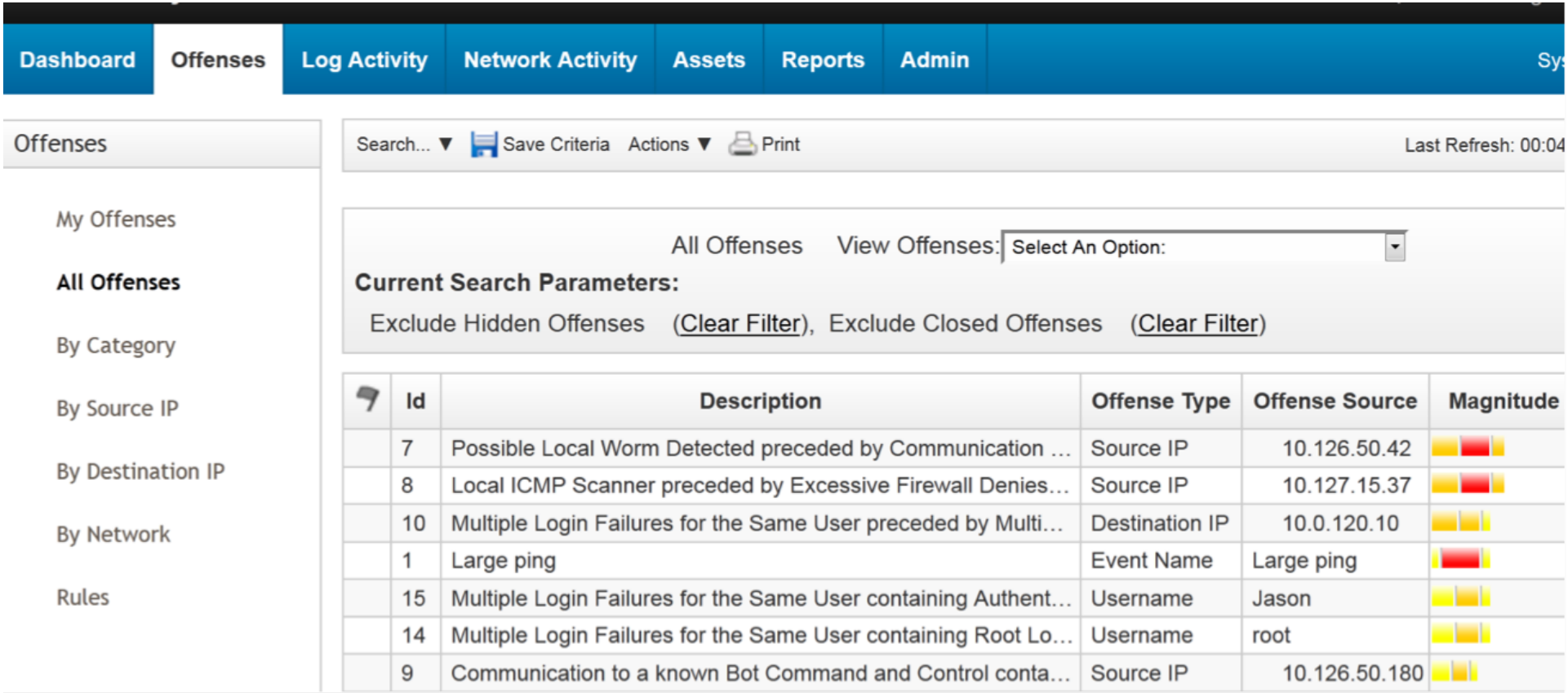
- Wie/warum verläuft die Kommunikation im Netzwerk von A -> B?



Source IP	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Application (Unique Count)
10.30.100.251	MNGT	Multiple (4)	Multiple (3)	MNGT	Multiple (3)
10.30.100.10	MNGT	Multiple (5)	Multiple (13)	MNGT	Multiple (5)
10.20.100.254	DMZ	Multiple (2)	Multiple (3)	DMZ	Multiple (4)
10.10.100.230	LAN	Multiple (7)	Multiple (5)	Multiple (4)	Multiple (7)
10.20.100.236	DMZ	Multiple (6)	Multiple (5)	Multiple (2)	Multiple (6)
10.10.100.254	LAN	Multiple (2)	Multiple (3)	LAN	Multiple (4)
10.10.100.45	LAN	Multiple (3)	443	other	SecurityProtocol.TLS
10.10.100.238	LAN	Multiple (2)	53634	Multiple (2)	DataWarehousing.drda
10.30.101.5	Net_10_0_0_0	10.30.101.3	Multiple (2)	Net_10_0_0_0	Multiple (2)
192.168.250.6	VPN-SSL	Multiple (5)	Multiple (6)	Multiple (2)	Multiple (10)

Offenses: Anomalitäten erkennen – JETZT!

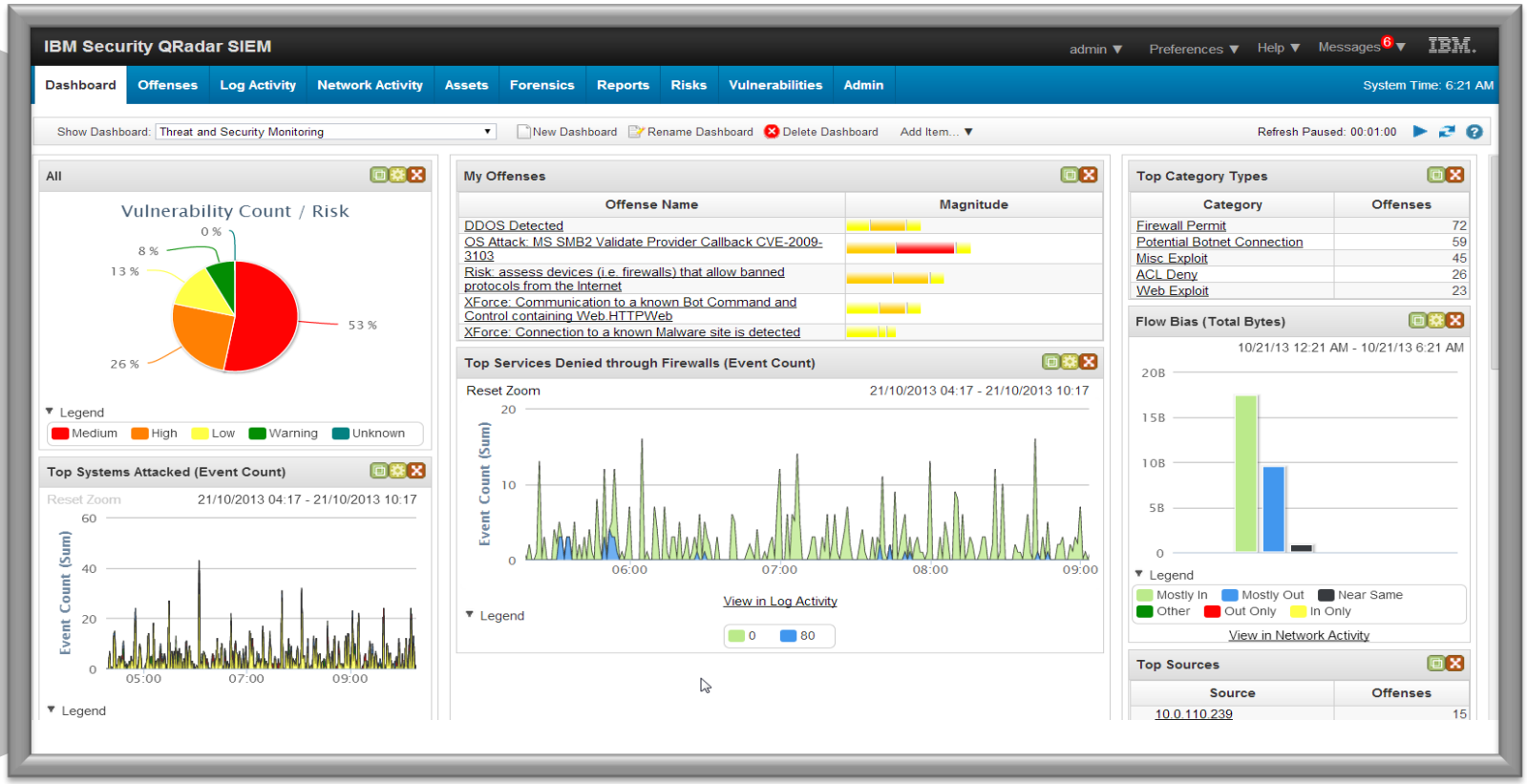
- Priorisierte Offense gezielt bearbeiten!



Id	Description	Offense Type	Offense Source	Magnitude
7	Possible Local Worm Detected preceded by Communication ...	Source IP	10.126.50.42	
8	Local ICMP Scanner preceded by Excessive Firewall Denies...	Source IP	10.127.15.37	
10	Multiple Login Failures for the Same User preceded by Multi...	Destination IP	10.0.120.10	
1	Large ping	Event Name	Large ping	
15	Multiple Login Failures for the Same User containing Authent...	Username	Jason	
14	Multiple Login Failures for the Same User containing Root Lo...	Username	root	
9	Communication to a known Bot Command and Control conta...	Source IP	10.126.50.180	

Verdichtung: Eine zentrale webbasierte Konsole mit Blick auf die gesamte IT

- Log Management
- Offenses
- Netzwerk Aktivitäten Monitoring
- Aktive Assets
- Schwachstellen Management
- Risiko Management



Verdichtung: Potentielle Angriffe erkennen

- Korrelieren von Events, Flows, Incidents relevanter Systeme

Optimierte Bedrohungs-Analyse

Tägl. Volumen von Events, Flows, Incidents

2,000,000,000

automatisch analysiert, um

20 – 25

potentielle Angriffe zu prüfen

Quelle: IBM

Zusammenfassung

- ✓ Bedrohungslage ist eindeutig
- ✓ Angriffe sind schonungslos und clever
- ✓ Klassische IT Sicherheit kommt an Grenzen
- ✓ IT Strategie ständig überprüfen und verbessern
- ✓ Die mobile Welt ist allgegenwärtig mit neuen Herausforderungen
- ✓ Intelligente Sensoren erkennen, was in unserem Netzwerk tatsächlich gerade passiert!
- ✓ **IT Sicherheit 2.0 sollte das Ziel der IT-Strategie sein**

Ziel - IT-Sicherheit 2.0

Stabilität durch Wandel
Wer nichts verändern will, wird auch das verlieren, was er bewahren möchte.

Dr. Gustav Walter Heinemann