Security Trends: Information Security Survey & Datenschutzgrundlage

Im Rahmen einer CON•ECT Informunity fand am 21. Februar 2017 die alljährliche Veranstaltung zum Thema »Security Trends« statt. Zahlreiche renommierte Referenten gaben mit Ihren Beiträgen einen Überblick über die aktuelle Thematik. Moderiert wurde die Veranstaltung von Krzysztof Müller (Executive Consultant, GRC bei NTT Security)

GSISS 2017 – Global State of Information Security Survey 2017

Christian Kurz (PwC)

Jahr für Jahr werden Cyber-Attacken häufiger, schwerwiegender und haben umfassendere Auswirkungen, gleichzeitig werden die Methoden zu deren Aufdeckung und Verhinderung sowie Innovationen im Bereich Cyber-Sicherheit ebenfalls verbessert. Führungskräfte wollen Lösungen, die die Cyber- Risiken verringern und die Unternehmens-Performance verbessern. Wie Manager mit Innovationen und Rahmenwerken zur Verbesserung von Sicherheit und Minimierung des Unternehmensrisikos umgehen, das zeigt die Global State of Information Security-Survey 2017, eine von PwC US zusammen mit dem CIO Magazine und CSO veröffentlichte Studie.

»Business E-Mail Compromise und Ramsonware haben die größten finanziellen Verluste 2016 verursacht.« – Christian Kurz (PwC)

Die PwC-Studie über den Zustand der Sicherheit ist eine gute Orientierung für die aktuellen Trends der Sicherheit. Sie zeigt auch deutlich, welche Aspekte der Sicherheit erhöhten Aufmerksamkeit benötigen. Diese Studie ist auch eine gute Grundlage, um die Datenschutz-Problemzonen zu identifizieren. Unter anderen erfahren wir aus der Studie, dass die Mehrheit der Datenverluste durch Zulieferer oder Partner verursacht worden sind. Diese Tatsache bedeutet, dass in der Umsetzung von EU-DSGVO das Thema Lieferanten- und Partner-Management eine besondere Aufmerksamkeit benötigt.

Resilient – Die hohe Kunst der Incident Response

Arne Jacobsen (IBM)

Security Incident Response Management gewinnt eine immer größer werdende Bedeutung für die IT-Security Strategie von Unternehmen und Behörden.

Die steigende Anzahl und zunehmende Komplexität von Angriffen stellt die Security Teams vor immer neue Herausforderungen. In dem Vortrag wurde aufgezeigt wie Incident Response Prozesse orchestriert, und automatisiert werden können, so dass schneller besser und nachhaltiger auf Angriffe und Cyber-Krisen reagiert werden kann.

»Ich bin in der letzten Zeit in vielen Firmen in Richtung Security unterwegs und es gibt ein sehr heterogenes Bild. Security kann man in drei Teile teilen: Prevention, Detection und Response.

Ich kann so gut es geht mein Netzwerk schützen – es wird immer einen Angreifer geben, der durchkommt.

SIEM-Technologien werden oft als Logdatengrab eingesetzt.«

»Resilient« ist eine Software, die sich als zentrale Plattform für incident response sieht.« – Arne Jacobsen (IBM)

Die EN 50600: Ein Mehrwert für das ISMS

Markus Hefler (Raiffeisen Informatik Center Steiermark)

Das europäische Gegenstück zur amerikanischen Data-Center-Norm ANSI/TIA 942 ist die EN 50600 Einrichtungen und Infrastrukturen von Rechenzentren und wurde mit Veröffentlichung des letzten Teils der Design-Gruppe »EN 50600–2–5 Security Systems« vollständig publiziert und bildet somit als erster europäischer Standard eine Grundlage für die Zertifizierung von Rechenzentren. Der Bereich Operations adressiert den sicheren RZ-Betrieb mit Unterstützung der nachgelagerten KPI. »Die Norm soll sich gut integrieren und auch einen Wert für das Management liefern.«

»Nur Prozesse ohne Rahmenbedingungen dokumentieren, ist aber im Fall des Vorfalls problematisch – vor allem wenn die Dokumentation nur online verfügbar ist.« – Markus Hefler (Raiffeisen Informatik Center Steiermark)

Die neue Datenschutzgrundverordnung

Dr. Christof Tschohl (Research Institute)

In diesem Vortrag wurden die Teilnehmer an die Thematik der Datenschutzgrundverordnungen und an die Grundlagen des Datenschutzes herangeführt.«Die Strafdrohungen sind natürlich der Turbobooster. Die Datenschutzgrundverordnung wird am 25.5.2018 rechtswirksam. Eine Verordnung braucht keine Umsetzung, sie gilt so, wie sie formuliert wurde.

Man haftet strafrechtlich nicht nur, wenn etwas passiert ist, es gibt auch ausdrücklich einen Katalog wenn wesentliche Handlungspflichten verletzt werden.

Zentral ist beim Datenschutz die Frage der Zweckbindung.

Podiumsdiskussion: Dr. Christof Tschohl (Research Institute), **Christian Kurz** (PwC), **Wolfgang Prentner** (ZT PRENTNER-IT), **Markus Hefler** (Raiffeisen Informatik Center Steiermark), **Arne Jacobsen** (IBM), **Krzysztof Müller** (Consultant) (v.l.n.r.)

Wenn ein Dienstleister seine Verarbeitung so intransparent macht, dass sie den Auskunftspflichten nicht nachkommen können, dann haften sie.

Manchmal kollidiert Datenschutz mit Datenschutz – Kundendaten vs. Mitarbeiterdaten.

»Wir werden mehr interdisziplinären Austausch brauchen. Privacy by Default.« – Dr. Christof Tschohl (Research Institute)

Cybersecurity trifft Safety – Bedrohung jenseits von Datenklau und Verletzung der Privatsphäre?

Erwin Schoitsch (AIT)

Wo sind die Zeiten hin, in denen selbst komplexe Systeme wie Industrieanlagen oder Transportsysteme übersichtlich, in sich geschlossen und abgegrenzt von der übrigen Cyber-Welt waren – mit eigenen Kommunikationssystemen, technischer Überwachung und Kontrolle durch eigenes, speziell geschultes Personal, im schlimmsten Fall mit einem Sicherheitszaun herum? Die hochgradige Vernetzung der Systeme zu Systems-of-Systems über die gängige IP-Netzwerksstruktur schafft viele neue Möglichkeiten – wurde aber nicht zugleich die Büchse der Pandora damit geöffnet?

Sicherheitstest für mobile Applikationen – Warum reines Vertrauen auf TLS/SSSL nicht genug ist

Peter Kieseberg (Kibosec)

Sicherheitstests sind ein fundamentaler Aspekt in vielen weit verbreitete Methoden des Software-Testings. Allerdings ist es oftmals der Fall, dass die eingesetzten Security-Protokolle nicht hinterfragt oder getestet werden. In diesem Vortrag gaben wir einen kurzen Überblick darüber, wie aufgrund dieser Praxis essentielle Sicherheitslücken im Rahmen von Sicherheitstests und der Qualitätskontrolle übersehen werden. Dabei konzentrieren wir uns auf zwei grundsätzliche Probleme: Die Definition eines korrekten und umfassenden Angreifermodells, sowie das Setzen von Vertrauen in den Client bei der Nutzung kryptographischer Algorithmen.

»Es ist essentiell sich vor der Entwicklung mit Fragen zum Angreifermodell, zum Schutzbedürfnis, aber auch der vertrauenswürdigen Entitäten zu beschäftigen.« – Peter Kieseberg (Kibosec)

Weitere Zitate unserer Vortragenden

Christian Kurz:
»Digitalization has impacted security spending.«
»41 % von den Security Incidents aus dem Jahr 2016 sind von Zulieferer verursacht.«

Arne Jacobsen:
»Die moderne Cybersecurity ist mehr als nur Prevention. Es gehört dazu auch Detection und Response.«

Marcus Helfer:
»Eine gute Abstimmung und Kommunikation zwischen IT-Betrieb und Facility Management ist entscheidend für reibungloses Funktionieren eines Rechnezentrums.«

Krzysztof Müller:
»Die zwei Haupttreiber für Security und Privacy: Angst und das Gesetz. Technologie ändert die Situation regelmäßig. Ansonsten wäre alles sehr stabil und die Aufgabe wäre erledigt.«

Papers und Folien

Die Papers bzw. Folien lönnen unter **www.paper4you.at** heruntergeladen werden.

papers 4you

AGENDA DER VERANSTALTUNG

GSISS 2017 – Global State of Information Security Survey 2017
Christian Kurz (PwC)

Resilient – Die hohe Kunst der Incident Response
Arne Jacobsen (IBM)

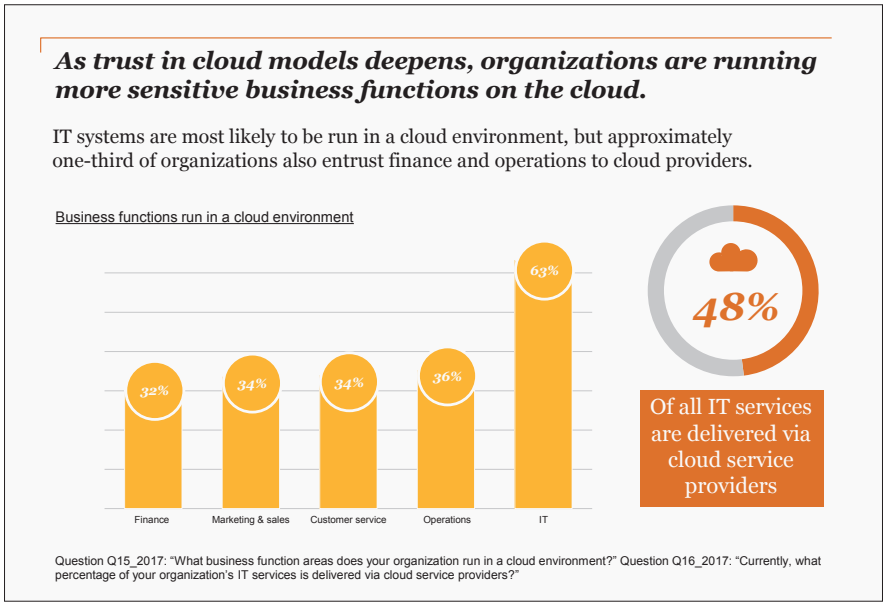
Die neue EU Datenschutzgrundverordnung
Dr. Christof Tschohl (Research Institute)

Podiumsdiskussion: zu aktuellen Trends des Global State of Information Security Survey 2017 und der EU Datenschutzgrundverordnung
mit: Arne Jacobsen (IBM), Markus Hefler (Raiffeisen Informatik Center Steiermark), Christian Kurz (PwC), Wolfgang Prentner (ZT PRENTNER-IT), Dr. Christof Tschohl (Research Institute)
Moderation: Thomas Bleier (Future Network Beirat) und Krzysztof Müller (Consultant)

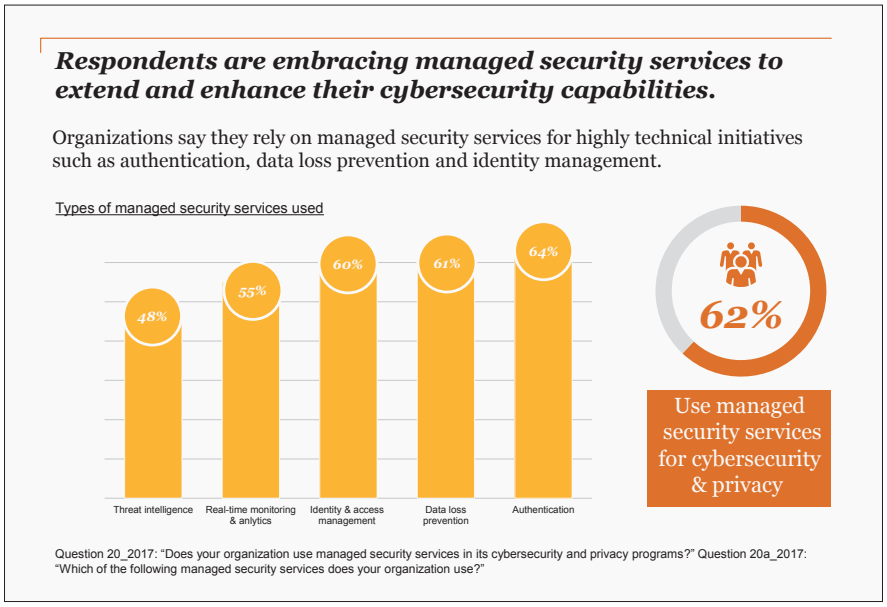
Cybersecurity trifft Safety – Bedrohung jenseits von Datenklau und Verletzung der Privatsphäre?
DI Erwin Schoitsch (AIT Austrian Institute of Technology GmbH)

Die EN 50600: Ein Mehrwert für das ISMS – Ein Erfahrungsbericht
Markus Hefler (Raiffeisen Informatik Center Steiermark)

Sicherheitstest für mobile Applikationen – Warum reines Vertrauen auf TLS/SSSL nicht genug ist
DI Peter Kieseberg (Kibosec GmbH)



Quelle: PwC

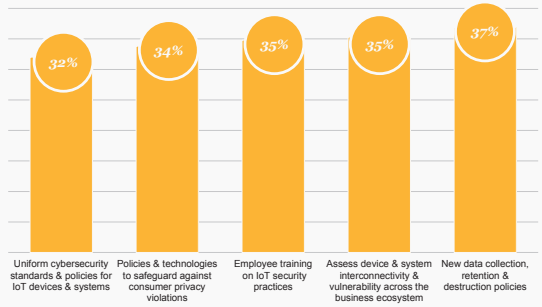


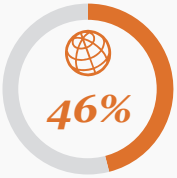
Quelle: PwC

As the Internet of Things takes off, organizations are moving to update their cybersecurity and privacy safeguards.

Key initiatives address data governance, device and system interconnectivity, and employee training. Consumer privacy is also a priority.

Policies, technologies & people skills being implemented for the Internet of Things





Are investing in a security strategy for the Internet of Things

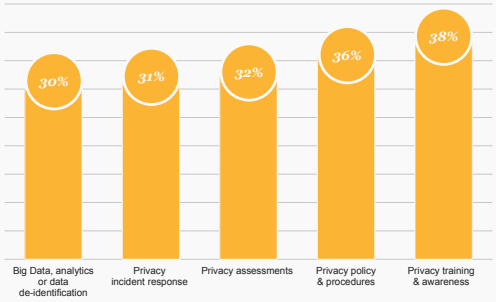
Question 25_2017: "What policies, technologies and people skills does your organization plan to implement over the next 12 months to address the cybersecurity and privacy risks associated with the Internet of Things (IoT)?" Question 10A_2017: "What types of security safeguards does your organization plan to invest in over the next 12 months?"

Quelle: PwC

As data privacy becomes an increasingly critical business requirement, employee training is a top priority.

Businesses are also updating privacy policies and procedures, and conducting privacy assessments.

Top privacy initiatives for 2016



Currently require employees to complete privacy training

Question 24_2017: "Which of the following projects, if any, will your privacy function address over the next 12 months?" Question 10a_2016: "Which safeguards does your organization currently have in place?"

Quelle: PwC

Our Unique Value

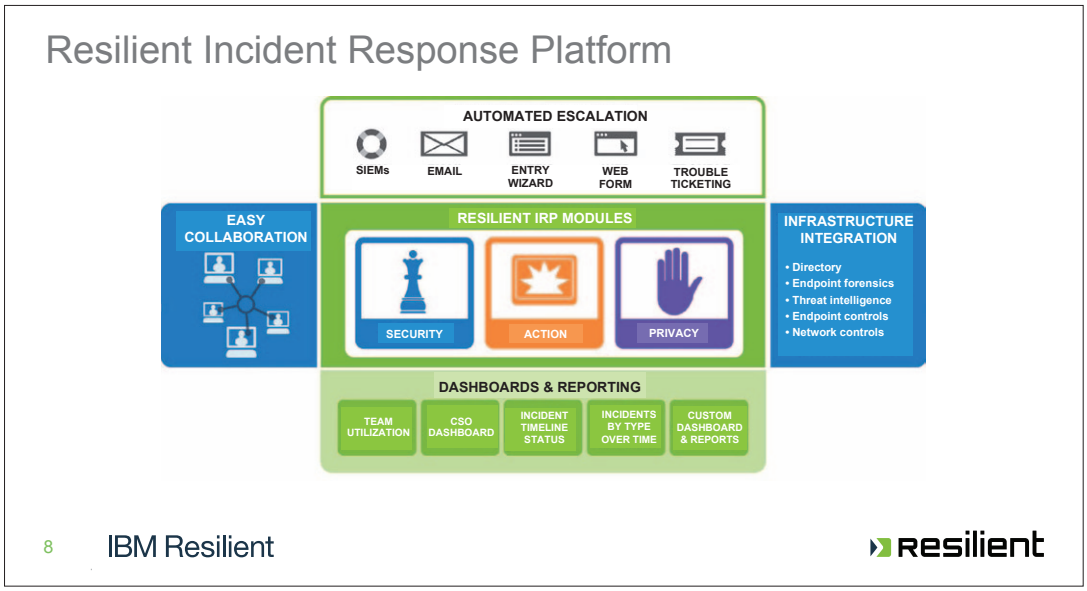
Resilient integrates with all existing security systems to create a single hub for IR transforming organizations' security posture.

- Aligns people, process, and technology across the organization
- Enables security teams to automate and orchestrate their IR processes
- Ensures IR processes are consistent, intelligent, and configured to teams' specific needs

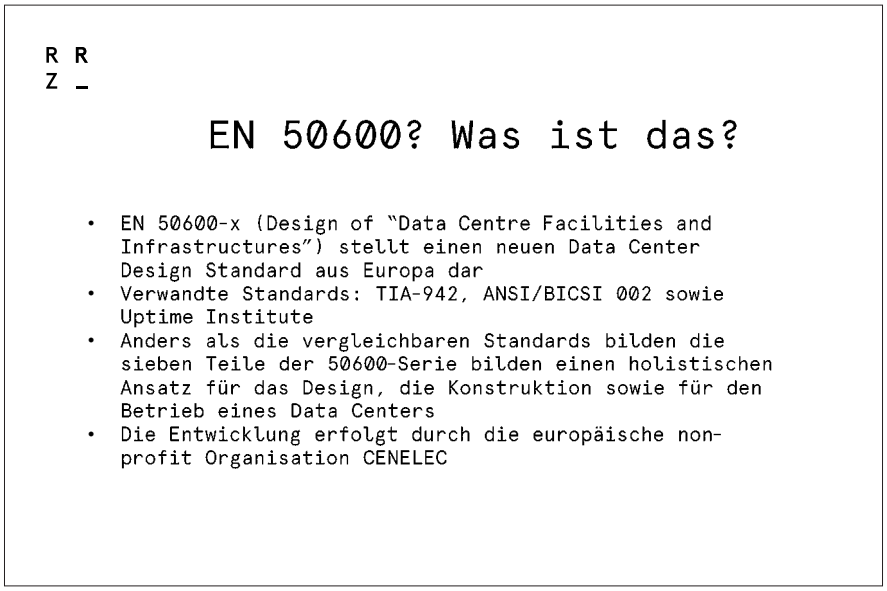
6 IBM Resilient

resilient

Quelle: IBM



Quelle: IBM



Quelle: Raiffeisen Informatik Center Steiermark

Die Veranstaltung wurde unterstützt von: