Mein Garten, mein Haus und meine Uhren

…was hat das mit IT-Sicherheit zu tun ?

Hamburg, 28. September 2015

Roland von Gehlen

Zu meiner Person…

Von Gehlen
Datenschutz und Datensicherheit
Pragmatisch – Einfach – Effizient

- ✓ Über 20 Jahre in leitenden IT-Linienfunktionen für verschiedene Unternehmen.
- ✓ Kenntnisse des IT-Business auf der Kundenseite in allen Facetten. Von der Anforderung des Fachbereiches bis zum stabilen 7x24h Betrieb
- ✓ Zusätzlich über fünf Jahre Erfahrung als zertifizierter Datenschutzbeauftragter und IT-Sicherheitsbeauftragter für die Otto Group (Otto GmbH & Co KG)
- ✓ Komme aus dem Handel und bevorzuge pragmatische, einfache Lösungen
- ✓ Stärke liegt in der Kommunikation zwischen Fachbereich und IT-Dienstleistern (Ich spreche beide „Sprachen“).
- ✓ Unabhängig und nicht an IT-Firmen gebunden. Ich agiere i.S. des Unternehmens
- ✓ Vernetzt mit einem Kreis von Spezialisten im IT-Sicherheitsumfeld und Juristen im Datenschutz- und Medienrecht (bis zur Uni Münster)

FEGRO SELGROS CASH & CARRY → JP JEAN PASCALE → OSP Otto Group Solution Provide → otto group →

Leiter IT-System-Planung	CIO	Geschäftsführer Retail	Bereichsleiter Einkauf + Retail	Direktor Software Development	Bereichsleiter Konzern Datenschutz + IT-Sicherheit

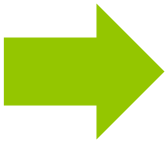
IT-Sicherheit in der heutigen Form ist relativ neu in der Geschichte

Von Gehlen
Datenschutz und Datensicherheit
Pragmatisch – Einfach – Effizient

Erst 1991 taucht der Begriff der IT-Sicherheit auf

Früher (90erJahre)

- Eigenes Rechenzentrum
- Terminals am Host
- Kaum Vernetzung
- Datensparsamkeit
- Feste Standorte eigner IT
- IT-Sicherheit gegen D.A.U.



Heute (2015 lt.Gartner Group)

- Cloud Computing
- Computing Everywhere
- Hohe Vernetzung (Internet der Dinge)
- Big Data
- Mobile Device Dritter
- IT-Sicherheit Against All

IT - Grundschutz im Unternehmen

„Noch nie betroffen“

„Wir nutzen Passwörter“

„Wir nutzen eine sichere MPLS-Leitung“

„Ich kenne alle Mitarbeiter“

„Wir haben eine Berechtigungsprüfung“

„Unser Virenscanner ist kostenlos“

„Der Server steht bei der GF im Zimmer“

Grundsicherheit im häuslichen Umfeld durchgängig vorhanden

- Es werden unterschiedliche Hemmschwellen eingebaut
- Awareness der Gäste und Bewohner wird erwartet (häusliche Richtlinie)
- Sie wissen um Ihre „Kronjuwelen“ im häuslichen Umfeld
- Man kann sich gegen alle möglichen Risiken versichern
- Das alles wird einem von Kindesbeinen an vermittelt

Aber wie sieht es mit dem Grundschutz IT-Umfeld aus?

Von Gehlen
Datenschutz und Datensicherheit
Pragmatisch – Einfach – Effizient

- ✓ **Grundsicherheit im persönlichen Umfeld durchgängig vorhanden**

Grundsicherheit im IT-Umfeld vorhanden?

Rechenzentrum im separaten closed-shop Betrieb – Arbeitsplatzrechner gesichert – Nicht jeder kann an jede Applikation – Berechtigungskonzept – Datenverschlüsselung – ausgelagertes Back-up?

- ✓ **Es werden unterschiedliche Hemmschwellen eingebaut**

Existieren unterschiedliche Hemmschwellen?

Vier-Augen-Prinzip – Need-know-Prinzip – Zweifaktor Authentifizierung – Logfile Auswertung

?

- ✓ **Kronjuwelen im häuslichen Umfeld sind bekannt und geschützt**

Sind die digitalen „Kronjuwelen“ bekannt?

- ✓ **Awareness der Gäste wird erwartet (häusliche Richtlinie)**

Awareness der Mitarbeiter vorhanden?

Richtlinien – geschult und verstanden – nachweislich!

- ✓ **„Man kann sich gegen alle möglichen Risiken versichern**

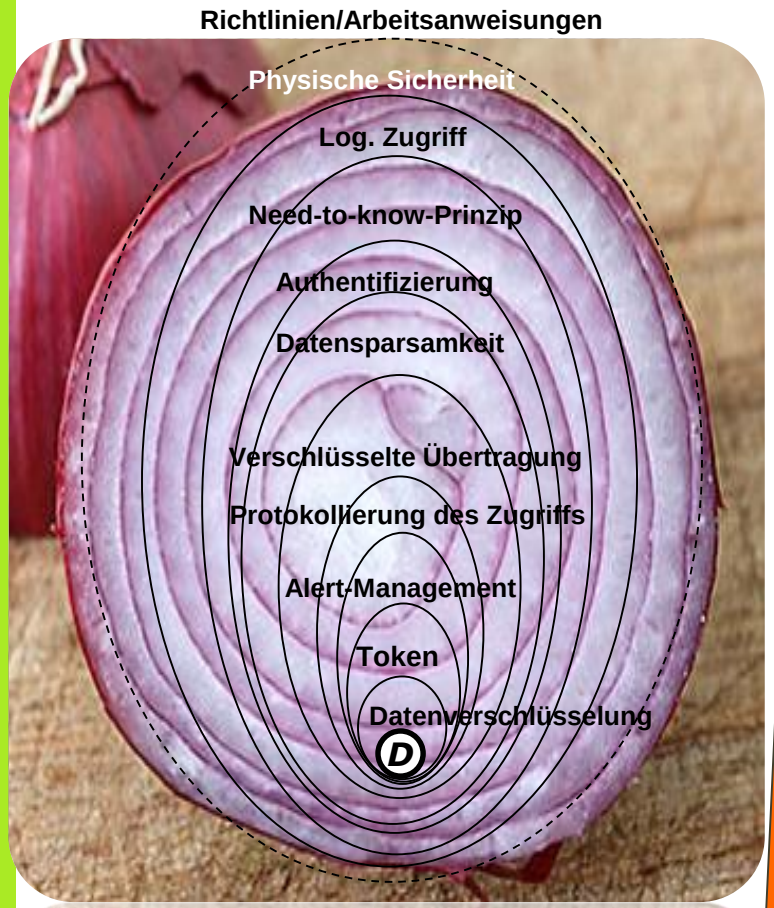
Kennen Sie Risikoversicherungen im IT-Umfeld ?

- ✓ **Das alles wird einem von Kindesbeinen an vermittelt**

<u>Nichts</u> davon ist uns in der IT-Sicherheit von Kindesbeinen vermittelt worden!

Nach dem „Zwiebelprinzip“© kann man auch hier den Grundschutz erhöhen!

Von Gehlen
Datenschutz und Datensicherheit
Pragmatisch – Einfach – Effizient



© „Zwiebelprinzip“ nach von Gehlen 2012

Sicherheit

1. Richtline/Arbeitsanweisungen
2. Physische Sicherheit
3. Logische Absicherung/Zugriff
4. Need-to-know Prinzip
5. Authentifizierung
6. Datensparsamkeit
7. Verschlüsselte Übertragung
8. Protokollierung der Zugriffe auf sensible Daten
9. Automatisierte zeitnahe Überwachung der Protokolle
10. Token /2-Faktor Authentifizierung
11. Datenverschlüsselung

Machen Sie selbst ein kurzes Selfaudit über die eigene IT-Sicherheit

Von Gehlen
Datenschutz und Datensicherheit
Pragmatisch – Einfach – Effizient

Richtline/Arbeitsanweisungen

- Wir haben IT-Sicherheitsrichlinien mit den wesentlichen Anweisungen für unsere Mitarbeiter und Dienstleister. — JA
- Unsere sensiblen Daten („Kronjuwelen“) sind definiert und den Bereichen bekannt. — JA
- Die Richtlinie(n) sind geschult und allen Mitarbeitern nachweislich bekannt. — JA

Physische Sicherheit

- Unser Rechenzentrum/Serverraum ist bei uns oder unserem Dienstleister im closed-shop gesichert. — JA
- Arbeitsplatzrechner sind gesichert. — JA
- Schnittstellen werden überwacht. — JA
- Es existiert ein funktionierendes, zeitnahes, physisch getrenntes Back-System. Restore wird (regelmäßig) getestet. — JA

Logische Absicherung/Zugriff

- Unser Netzwerk ist segmentiert und durch Firewalls sinnvoll eingeteilt und getrennt. — JA

Need-to-know Prinzip

- Nur derjenige, der einen Zugriff auf eine Applikation für seinen Job braucht, kann auf die Applikation zugreifen — JA

Authentifizierung

- Wir haben ein Rollen- und einem Berechtigungskonzept für unsere IT-Systeme und die Vergabe ist nach dem 4-Augen-Prinzip gesichert — JA

Datensparsamkeit

- Wir hinterfragen die Speicherung von sensiblen Daten
- Wir haben ein Löschkonzept für nicht mehr benötigte Daten — JA

Verschlüsselte Übertragung

- Daten werden (zumindest nach extern) nur über gesicherte Protokolle, wie z.B. HTTPS/SFTP/VPN übertragen. — JA

Protokollierung der Zugriffe

- Zugriffe auf sensible Daten werden revisionssicher (unveränderbar) geloggt und.. — JA

Automatisiert, zeitnah überwacht

- Die Logfiles von Zugriffen auf sensible Daten werden automatisiert überwacht und mit Hilfe von Alert-Regeln ausgewertet. — JA

Token /2-Faktor Authentifizierung

- Für sensible Bereiche existiert eine zusätzliche dynamische Identifikation — JA

Datenverschlüsselung

- Sensible, unternehmenskritische Daten werden verschlüsselt gespeichert — JA

Haben Sie zu wenig „JA- Kreuze oder noch Fragen, rufen Sie mich an oder schreiben mir

Von Gehlen
Datenschutz und Datensicherheit
Pragmatisch – Einfach – Effizient

Lassen Sie sich dabei helfen, Ihre betriebliche Datensicherheit und Ihren Datenschutz smart umzusetzen. Ich unterstütze Sie dabei, die vielfältigen Anforderungen im Umgang mit sensiblen Daten zu effizient zu erfüllen, Ihre Mitarbeiter zu sensibilisieren und die notwendigen technischen und organisatorischen Maßnahmen umzusetzen.

…und das ohne das Business auszubremsen.

Roland von Gehlen
Alte Landstraße 220
22391 Hamburg

Roland@von-gehlen.com
+49 40 532 67 888
+49 172 43 43 47 2
XING: Roland von Gehlen

Ich freue mich, wenn ich Sie dabei unterstützen darf