Sicherheit 3.0

Der Weg von Perimeter-Sicherheit zur Informationssicherheit

MÜNCHNER KREIS

Dr. Laura Georg

Impulsvortrag

Inhalt

Neue Geschäfts- und Arbeitsmodelle treiben den Wandel in der IT voran.

Unternehmen können mehr potentielle Kunden erreichen und mehr mit bestehenden Kunden kommunizieren

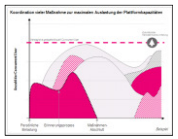
- Facebook
- Twitter

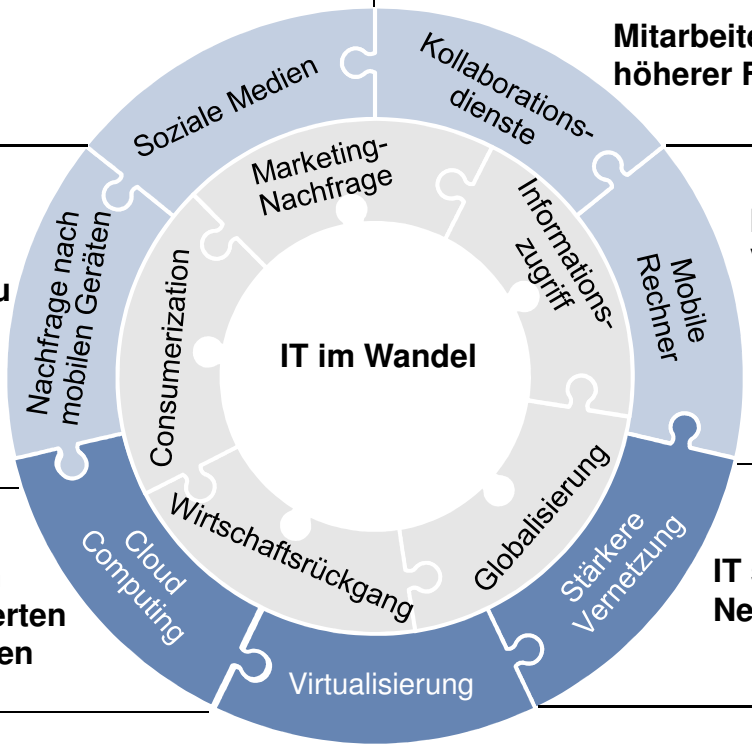
Mitarbeiter wollen Kollaborationsdienste um Aufgaben und Dokumente effizienter zu bearbeiten

Mitarbeiter arbeiten von zu Hause, zwecks höherer Flexibilität und Kosteneinsparungen

Führungskräfte und Mitarbeiter erwarten eigene/trendige Mobiltelefone und Tablets auch in ihren Unternehmen nutzen zu können

Remote Nutzer zwingen die IT Informationen auch online verfügbar zu machen





Unternehmensdienstleistungen können günstig auf cloud-basierten Internet-Servern gehostet werden

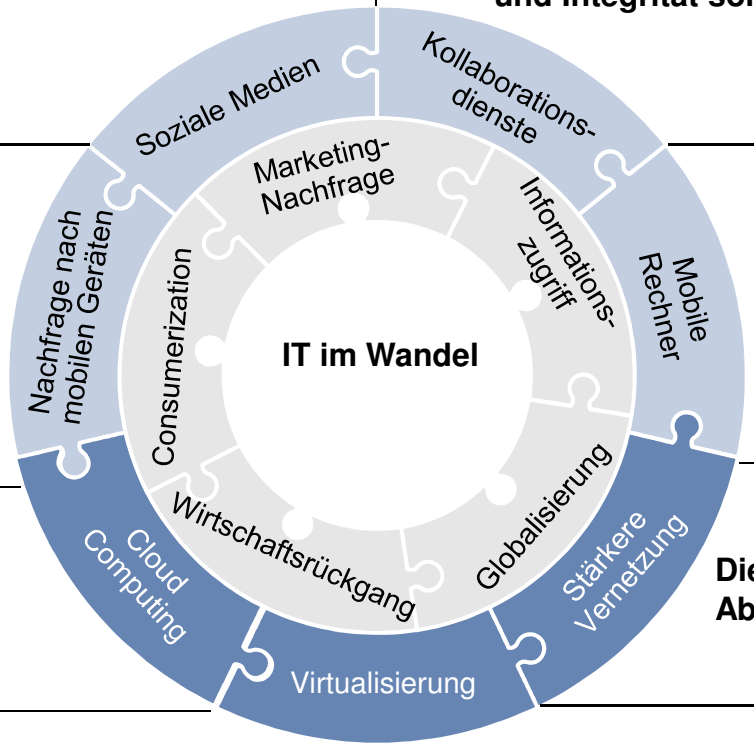
IT steigert die Konnektivität zu mehr Netzwerken für Partner und Kunden

Server die viele Anwendungen hosten erzielen Kosteneinsparungen

Was bedeutet das für die IT-Sicherheit in den Unternehmen?

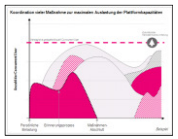
Posts von Mitarbeitern in sozialen Medien reflektieren die gesamte Reputation des Unternehmens

Daten werden abgerufen, geteilt und verändert. Die IT muss sicherstellen, dass die Vertraulichkeit und Integrität solcher Daten gewährleistet ist



Die Herrschaft über Betriebs- und Applikationssicherheit ist gefährdet

Die Möglichkeit von Datenverlusten nimmt zu



Firmendaten sind über Unternehmensgrenzen hinweg gespeichert

Die Angriffsfläche wächst, sowie die Abhängigkeit von Dritten

Ein kompromittierter Server kann viele Systeme gefährden

Wie betreffen die Unternehmen diese Veränderungen?

Attacken geschehen täglich

*"***Amazon** hatte eine kryptographische Schwäche in ihren EC2- und S3-Diensten, die es Hackern erlaubte Kundenkonten auszuspähen – diese konnte behoben werden."
Quelle: SCMagazine

"Die Hotelkette **Travelodge** räumte ein, dass ihre Kundendatenbank, die in der Cloud gespeichert ist, gehackt wurde und dass Kundendaten kompromittiert worden sind."
Quelle: thecloudcircle.com

*"***Sony Corp.** wurden 100 Millionen Kundendatensätze von ihrem PlayStation-Cloud-Netzwerk gestohlen.*"*
Quelle: Reuters

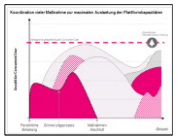
*"*Lulz Hackers, die ihre Angriffe auf ihrer eigenen Website und via Twitter bekannt machen, sagten am Freitag sie hätten Kundendaten von rund 200.000 Nutzern des Online-Video-Spiels Brink gestohlen.*"*
'Quelle: Reuters

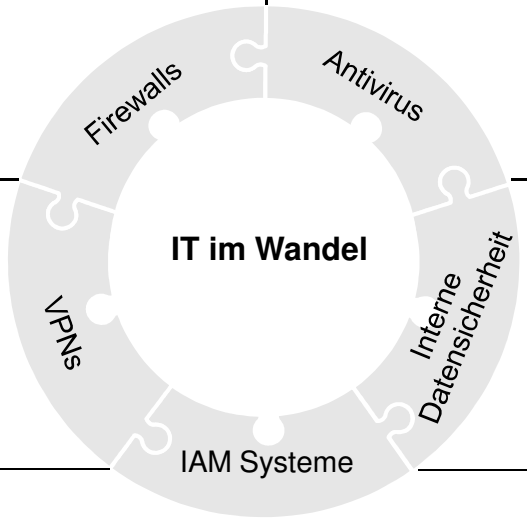
"Ein **BP**-Mitarbeiter hat nach der Golf-Ölpest einen Laptop mit persönlichen Daten von Tausenden von Personen, die Schadensersatzanspruch angemeldet haben, verloren, wie ein Sprecher des Unternehmens mitteilte."
Quelle: dailymail.co.uk

Welche Mechanismen werden den Risiken heute entgegengesetzt?

Viele Geschäftsprozesse durchdringen Netzwerkgrenzen, genau wie viele Internetprotokolle zunehmend durch Firewalls getunnelt werden

Neue APTs haben gezeigt, dass einfacher Antivirusschutz nicht mehr ausreichend für Firmen ist





Traditionelle VPNs sind nicht mehr erforderlich für die Bereitstellung der Konnektivität zu mobilen Endgeräten und Remote-Benutzern

Daten werden noch intensiver geteilt/ausgetauscht und traditionelle Rollenkonzepte sind nicht mehr ausreichend um Daten zu schützen

Aktuelle IAM-Systeme erweitern Authentifizierungs- und Autorisierungsmethoden nicht nur auf Remote-Benutzer und Netzwerke

Was bedeutet dies für unsere IT-Sicherheitsstrategie 3.0?

Der Schutz der Daten selber ist notwendig

- Unternehmen, Wirtschaft und Mitarbeiter sind die treibende Kraft weg von traditionellen IT-Mitteln

Authentifizierungsmechanismen müssen verstärkt werden

- Es gibt keine schützende räumliche Dimension mehr, die Sicherheit garantiert

1. **Die Verschlüsselung von als kritisch klassifizierten Daten ist ganzheitlich umzusetzen.**
2. **Der Schutz von Informationen muss unabhängig von Netzwerken und Systemen sein; „die Daten selbst müssen den Zugang kontrollieren“ (Daten-Authentifizierung).**
3. **Alle Systeme müssen resistent gegenüber Gefahren aus dem Internet sein und somit die Fähigkeit besitzen in andere Umgebungen bewegt werden zu können.**

Datensicherheit kann nicht mehr allein auf den Schutz der zentralen Systeme aufbauen.

Kontakt

Dr. Laura Georg
Head IT Risk & Security Management

Phone: +41 43 888 65 50
Mobile: +41 79 484 94 10
e-Mail: Laura.Georg@detecon.com

Detecon (Schweiz) AG

Löwenstrasse 1
8001 Zürich · Schweiz
Phone +41 43 888 65 00
Fax +41 43 888 65 10

www.detecon.com
Information.security@detecon.com

Detecon International GmbH

Oberkasseler Straße 2
53227 Bonn · Deutschland
Phone +49 228 700 0
Fax +49 228 700 3789

We make ICT strategies work