Kompass der IT-Sicherheit

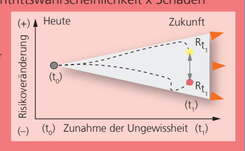
www.sit.fraunhofer.de

Fraunhofer SIT

zeitrelevant — bedingte, abhängige Wahrscheinlichkeit

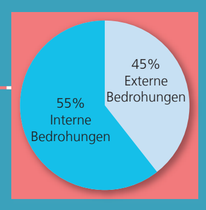
Risiko = Eintrittswahrscheinlichkeit x Schaden

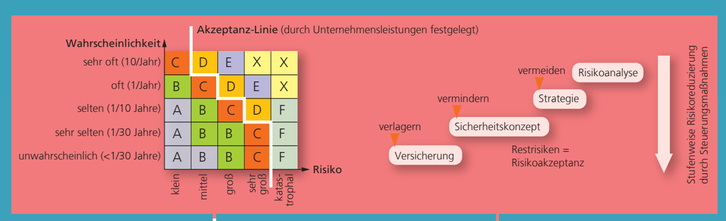
PROBLEM:
Sehr seltene, aber sehr große Schadensereignisse können als unbedeutendes Risiko betrachtet werden

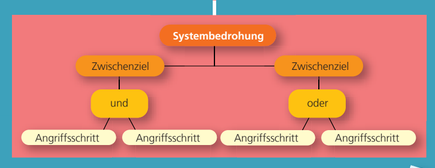


VISHING = VOIP + PHISHING

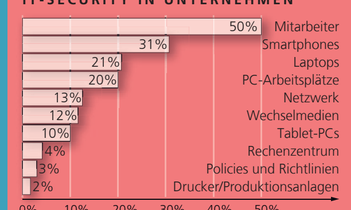
Durch automatisierte Telefonanrufe wird versucht, den Empfänger irrezuführen und zur Herausgabe von Zugangsdaten, Passwörtern, Kreditkartendaten usw. zu bewegen.







GEFÜHLT SCHWÄCHSTE GLIEDER DER IT-SECURITY IN UNTERNEHMEN



Quelle: IDC 2011

DATENSCHUTZRECHT

Generelles Verbot, personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen (§4 Abs. 1 BDSG) = Regel

Ausnahmen:
- Sie ist durch das BDSG oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet
- Wenn der Betroffene in die Verarbeitung einwilligt. Einwilligungserfordernis des Nutzers gemäß §3 Abs. 1-7

HAFTUNG/VERANTWORTLICHKEIT FÜR INTERNETINHALTE

- Volle Haftung für eigene Informationen (§7 Abs. 1 TMG)
- Haftung für fremde Inhalte: Haftungsprivilegien für
  - Accessprovider (§8 Abs. 1 TMG)
  - Cachingprovider (§9 TMG)
  - Hostingprovider (§10 TMG)

BGB, MarkenG, Strafgesetzbuch, UrheberrechtsG, UWG, PreisangabenVO, ...

URHEBERRECHT

§11 UrhG: Das Urheberrecht schützt den Urheber in seinen geistigen und persönlichen Beziehungen zum Werk und in der Nutzung des Werkes. Es dient zugleich der Sicherung einer angemessenen Vergütung für die Nutzung des Werkes.

§15 UrhG: Nur der Urheber hat das Recht, sein Werk in körperlicher Form zu verwerten; das Recht umfasst u.a. das Vervielfältigungsrecht, Verbreitungsrecht, das Vorführungsrecht und das Recht der öffentlichen Zugänglichmachung (§ 19a).

§97 UrhG: Wer das Urheberrecht widerrechtlich verletzt, kann von dem Verletzten auf Beseitigung der Beeinträchtigung, bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden und ist dem Verletzten zum Ersatz des daraus entstehenden Schadens verpflichtet.

UNSERE KOMPETENZFELDER

MOBILE SYSTEMS

Der Einsatz mobiler Geräte in Unternehmen birgt Gefahren. Fraunhofer SIT besitzt Erfahrung mit iOS, Android und weiteren Betriebssystemen. Die Mitarbeiter des Instituts entwickeln Lösungen, härten mobile Systeme, bewerten Produkte und unterstützen Unternehmen und Behörden mit umfangreichem Know-how.
www.sit.fraunhofer.de/mobilesystems

CLOUD COMPUTING

Um die Potenziale des Cloud Computing zu nutzen, brauchen Unternehmen Sicherheit hinsichtlich Compliance und technischen Risiken. Fraunhofer SIT entwickelt sichere, datenschutzkonforme IT-Anwendungen für die Cloud und berät Unternehmen bei der sicheren Gestaltung und Nutzung von Cloud-Angeboten.
www.sit.fraunhofer.de/cloudcomputing

SECURE ENGINEERING

Die Entwicklung von Software ist komplexen Prozessen mit vielen Akteuren unterworfen. Fraunhofer SIT entwickelt und optimiert standardisierte Engineering-Methoden, durch die ein vorhersagbares Maß an IT-Sicherheit erzeugt werden kann.
www.sit.fraunhofer.de/secureengineering

IDENTITY AND PRIVACY

Datenschutzskandale sorgen regelmäßig für großes Aufsehen. Die betroffenen Unternehmen erleiden dann oft Kundenabwanderungen, Umsatzeinbußen und Vertrauensverlust bei Geschäftspartnern. Fraunhofer SIT unterstützt Unternehmen und Behörden beim rechtssicheren und effizienten Umgang mit sensitiven Daten und beim Schutz von Informationen und Identitäten.
www.sit.fraunhofer.de/identityprivacy

SECURITY TESTLAB

Wie sicher die IT ist, stellt sich erst heraus, wenn sie von einem Angreifer ins Visier genommen wird. Das Testlabor des Fraunhofer SIT liefert frühzeitig Informationen über die Sicherheit eines Produkts oder Dienstes. Erfüllen diese die Sicherheitsanforderungen, können Unternehmen das mit einem Testat des Fraunhofer SIT belegen.
www.sit.fraunhofer.de/securitytestlab

MEDIA SECURITY

Digital produzierte und verteilte Medien sind anfällig für unberechtigte Zugriffe von außen oder illegale und unbemerkte Weitergabe durch Mitarbeiter. Fraunhofer SIT setzt zum Schutz digitaler Medien auf die Markierung durch digitale Wasserzeichen, mit denen sich Medien eindeutig kennzeichnen und zurückverfolgen lassen.
www.sit.fraunhofer.de/mediasecurity

CYBER-PHYSICAL SYSTEMS

Ob Auto oder Produktionsanlage, Cyber-Physical Systems und eingebettete Systeme sind Innovationstreiber und verarbeiten auch sicherheitskritische Daten. Das macht diese Systeme für Angreifer zu attraktiven Zielen. Fraunhofer SIT beschäftigt sich mit Sicherheit und Datenschutz von Cyber-Physical Systems und deren Kommunikationskanälen.
www.sit.fraunhofer.de/cyberphysicalsystems

IT FORENSICS

Viele Kriminelle nutzen heute Computer und Internet für ihre Zwecke. Oft hinterlassen sie dabei digitale Spuren. Diese Spuren zu erkennen, sicherzustellen und auszuwerten ist Aufgabe der IT-Forensik. Das Fraunhofer SIT bietet IT-forensische Analysen, Forensic Hacking, Mobile Forensics, Forensische Finanzdatenanalyse, File Carving und mehr.
www.sit.fraunhofer.de/itforensics

SECURITY MANAGEMENT

Heute reicht es nicht mehr, die eigenen Informationen nur mit technischen Lösungen wie Firewalls zu schützen. Fraunhofer SIT unterstützt Unternehmen bei Risikobewertung und -management mit Beratung, Konzepten sowie der Planung und Realisierung zielgruppenorientierter Trainingsmaßnahmen und Awarenesskampagnen.
www.sit.fraunhofer.de/securitymanagement

Industrie 4.0

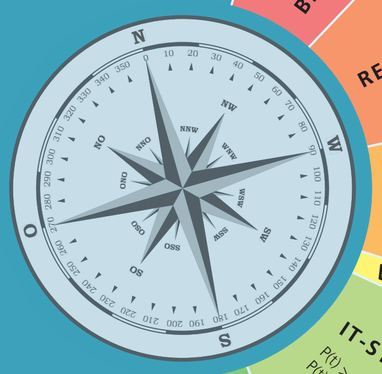
Die vierte Phase der Industrialisierung ist gekennzeichnet durch Vernetzung und Flexibilisierung. IT und IT-Sicherheit werden immer wichtiger. Fraunhofer SIT entwickelt Technologien, die diese Kommunikation schützen. Diese Lösungen beinhalten hardwarebasierte Sicherheit, Protokolle, Security Management sowie Monitoring.
www.sit.fraunhofer.de/industrie4.0

ANGRIFFSKLASSEN

- Buffer Overflow: Überschreiben von interpretierten Speicherbereichen
- Injection: Ändern der Semantik durch zusätzliche Befehlszeichen
- Race Conditions: Ausnutzen von Zeit-/Ereignisabhängigkeiten
- Brute Force: Durchprobieren des Eingaberaums
- Denial of Service: Verhindern der Nutzung
- Network Exploitation: Ausnutzen von Netzwerkeigenschaften z.B. Scanning, Sniffing, Replaying, Spoofing, Flooding, Bouncing, …
- Social Engineering: Ausnutzen menschlicher Schwächen

ANGREIFERMODELL

Ziel: Was will der Angreifer?
Motivation: Warum?
Fähigkeiten: Was kann der Angreifer?
→ Ökonomie: Gibt es eine »lohnende« Kombination für den Angreifer unter Risikoberücksichtigung?



SCHWACHSTELLEN, BEDROHUNGEN, ANGRIFFE

Identitätsdiebstahl, Phishing, Vishing, Spoofing, Pharming, Spam, Trojaner, Viren, Würmer

Angriffsklassen, Höhere Gewalt, Risiko- und Bedrohungsanalyse, Vortäuschung falscher Identität, Sabotage/Malware

REGELUNGEN UND GESETZE

Strafrecht, Zivilrecht, TK-Recht, KonTraG (Kontrolle und Transparenz im Unternehmensbereich), BDSG (Bundesdatenschutzgesetz), Finanzrechtliche Auflagen, Wettbewerbsrecht, Handelsrecht, Arbeitsrecht

MaRisk (Mindestanforderungen an das Risikomanagement), Euro SOX, SOX (Sarbanes Oxley Act), Basel II und Solvency I

SICHERHEITSMANAGEMENT

Awareness, Identitätsmanagement, Informations- und Zugriffskontrollmanagement, Sicherheitsprozesse

Account- und Passwort-Management, Digitale Identitäten, Role Based Access Control, User Provisioning/E-Provisioning, Mandatory Access Control, Zugriffsmatrix, Discretionary Access Control, Incident Management, Auditing, Monitoring, BCM, Emergency Response, Umsetzung der IT-Sicherheitsrichtlinien

WIRTSCHAFTLICHKEIT

Physische Sicherheit, Risikomanagement, Kosten, Schäden

IT-STRATEGIE

$P(t) > D(t) + R(t)$ ✓
$P(t) \leq D(t) + R(t)$ ↯

IT-SICHERHEITSPOLICY / -LEITLINIE

D: Erkennen, Schnittstellen

P: Schutzniveau

R: Reagieren

Materielle Schäden, Immaterielle Schäden, Antiviren-Scanner, Logfile-Analyse, IDS (Intrusion Detection System), Sicherheitsanalyse/Penetrationstest, Operatives Risikomanagement, ISO2700x, ITIL (IT-Infrastructure Library), CobiT, BCM (Business Continuity Management), ITSCM (IT-Service Continuity Management), VPN (Virtual Personal Network), VoIP (Voice Over IP), IPS (Intrusion Prevention System), Firewall, Backup-Konzept, Hardening Application, Schutz mobiler Endgeräte, Betriebssystem-Härtung, Incident Management, Emergency Response

Datenschutz, Datensicherheit

Vertraulichkeit, Privatsphäre, Verbindlichkeit, Authentizität, Verfügbarkeit, Integrität

Das Zusammenwirken von Schutzniveau und technischen und organisatorischen Maßnahmen beim Erkennen und Reagieren ist ein Maßstab für die Güte der IT-Sicherheit.

BDSG

Regelt zusammen mit den Datenschutzgesetzen der Bundesländer und anderen bereichsspezifischeren Regelungen den Umgang mit personenbezogenen Daten, die in IT-Systemen oder manuell verarbeitet werden.

§13 TMG — Pflichten des Diensteanbieters

DATENSCHUTZ IM ONLINEBEREICH

- Telekommunikationsgesetz §89 TKG
- Telemediengesetz §§11-15a TMG
- BDSG für datenschutzrelevante Inhalte von E-Mails

Alle Angaben über eine bestimmte oder bestimmbare natürliche Person sind personenbezogene Daten; besondere Arten siehe §3 Abs. 9 BDSG

SOX

Ein US-Gesetz zur verbindlichen Regelung der Unternehmensberichterstattung infolge der Bilanzskandale von inländischen und ausländischen Unternehmen, deren Wertpapiere an US-Börsen gelistet sind.

Verbindliche Vorgabe der Bundesanstalt für Finanzdienstleistungsaufsicht für die Ausgestaltung des Risikomanagements in deutschen Kreditinstituten.

KONTRAG

Präzisiert und erweitert hauptsächlich Vorschriften des HGB (Handelsgesetzbuch) und des AktG (Aktiengesetz). Kern des KonTraG ist eine Vorschrift, die Unternehmensleitungen dazu zwingt, ein unternehmensweites Früherkennungssystem für Risiken (Risikofrüherkennungssystem) einzuführen und zu betreiben, sowie Aussagen zu Risiken und Risikostruktur des Unternehmens im Lagebericht des Jahresabschlusses der Gesellschaft zu veröffentlichen.

§93 AktG

Aktiengesetz; Vorstandsmitglieder sind persönlich haftbar, wenn sie keine/unzureichende Vorsorge bzw. Frühwarnung im Rahmen des betrieblichen Risikomanagements betreiben.

AWARENESS

Awareness beschreibt Maßnahmen des IT-Sicherheitskonzepts, die es ermöglichen bewusst und souverän zu agieren.

KONTROLLMANAGEMENT

Als Kontrollhilfe sind Methoden (Software/Hardware) vorhanden, die die Authentifizierung überwachen.

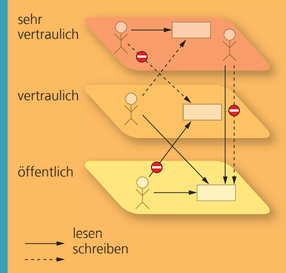
PASSWORTVERWALTUNG

Festlegung des Passwortkonzeptes
Passwort: La83%hge0
- ☑ Mindestlänge von 8 Zeichen
- ☑ Mindestens 1 Großbuchstabe und 1 Sonderzeichen
- ☑ Kein Eigen- oder Programmname
- ☑ Keine trivialen Tastaturzeichenfolgen
- ☑ Kein Begriff aus dem Wörterbuch

www.imobilesitter.de

MULTILEVEL SECURITY SYSTEM (MLS)

Beschränkung des Informationsflusses



BELL-LAPADULA

Festlegung der Zugriffsrechte basierend auf Systemregeln und Eigenschaften.

- Einfache Regel (Simple Security Property): »nicht nach oben lesen«
- Sternregel (*-Property): »nicht nach unten schreiben«

Rolle <> Rechte

Netz: Bell-LaPadula, Sichere E-Mails, Kerberos, IPsec, SSL/TLS, VPN & sichere Protokolle

S/MIME, PGP

Standards für den Schutz von E-Mails. Das meistgenutzte Kommunikationsmedium muss gegen mögliche Angriffe geschützt werden.

zur Authentifizierung

mächtigstes Protokoll zum Schutz von Verbindungen

DISCRETIONARY ACCESS CONTROL

Die Zugriffsrechte für (Daten-)Objekte werden pro Benutzer festgelegt.

WER DARF WAS?

Hierbei wird entschieden, ob auf eine Ressource zugegriffen werden darf. Die Zugriffsrechte müssen festgelegt und kontrolliert werden. Am geläufigsten ist dieses Konzept bei Dateisystemberechtigungen, wo festgelegt wird, welche Benutzer welche Dateien und Verzeichnisse lesen, schreiben, ändern oder ausführen dürfen. Vor allem dazu geeignet, die Vertraulichkeit, Integrität, Verfügbarkeit und Konsistenz von Daten zu sichern.

KOSTEN

Versicherung, Betrieb, Aufrechterhaltung, Mitarbeiterschulung

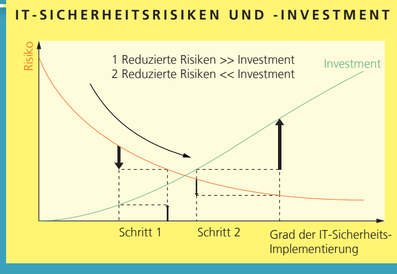
MATERIELLE SCHÄDEN

Vertragsstrafe, Haftung, Produktionsausfall

IMMATERIELLE SCHÄDEN

Verlust der Reputation sowie Vertrauensverlust bei Kunden und eigenen Mitarbeitern.

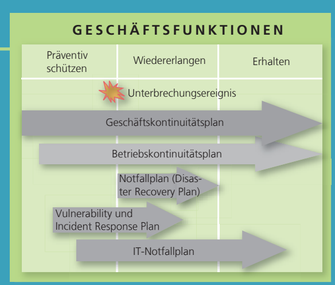
IT-SICHERHEITSRISIKEN UND -INVESTMENT



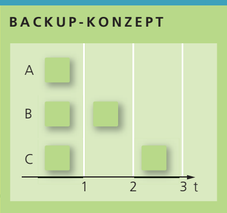
KONTINUITÄTSMANAGEMENT

Business Continuity Management ist der Aufbau eines leistungsfähigen Notfall- und Krisenmanagements zwecks systematischer Vorbereitung auf die Bewältigung von Schadensereignissen. So werden wichtige Geschäftsprozesse selbst in kritischen Situationen und in Notfällen nicht oder nur temporär unterbrochen und die wirtschaftliche Existenz des Unternehmens bleibt trotz Schadensereignisses gesichert.

GESCHÄFTSFUNKTIONEN



BACKUP-KONZEPT



Vollsicherung zum Zeitpunkt
2: A+B+C wird gesichert
3: A+B+C wird gesichert

Inkrementelle Sicherung zum Zeitpunkt
2: B wird gesichert
3: C wird gesichert

Differentielle Sicherung zum Zeitpunkt
2: B wird gesichert
3: B+C wird gesichert

Zum Zeitpunkt 1 wird eine vollständige Datensicherung durchgeführt. Kästchen markieren die Änderung einer Datei.

ZAHLEN, DATEN, FAKTEN

Entwicklung der Spam-Zahlen
weltweit, Symantec
http://sit4.me/symantec-spam

Entwicklung der Phishing-Zahlen
weltweit, Symantec
http://sit4.me/symantecphishing

Die Entwicklung von Schadsoftware
Microsoft, 10-Jahres-Bericht
http://sit4.me/microsoftreport

Halbjährliche Trend-Analayse zu Phishing
weltweit, Microsoft
http://sit4.me/microsoftphishing

Karte der Botnet-Aktivitäten
weltweit, Symantec
http://sit4.me/symantecbotnets

Monatlicher Report zu Onlinebetrug
RSA
http://sit4.me/rsaonlinebetrug

Halbjährliche Trend-Analyse von Botnet-Aktivitäten
Deutschland, Microsoft
http://sit4.me/microsoftbotnet

Wie wird IT-Sicherheit in Unternehmen wahrgenommen?
PwC, CIO Magazine, CSO Magazine
http://sit4.me/itsicherheit

Jahresbericht des Bundeskriminalitätsamts zur Wirtschaftskriminalität
http://sit4.me/bkawirtschaft

Jahresbericht des Bundeskriminalamts zur Internetkriminalität
http://sit4.me/bkacybercrime

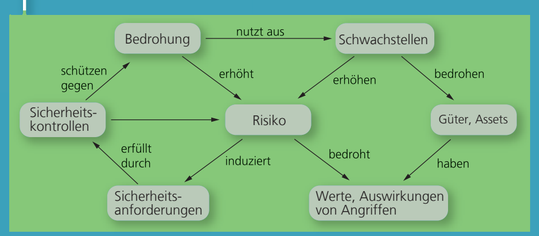
Monatliche Entwicklung der Viren-Zahlen
weltweit, Symantec
http://sit4.me/symantecviren

Halbjährliche Trend-Analyse zu Malware
weltweit, Microsoft
http://sit4.me/microsoftmalware

CLOUD-SPEICHER-SICHERHEIT

- Sichere Datenverlüsselung
- Transportsicherheit
- Datenschutz bei Deduplication
- Risiko Provider-Lock-In
- Sicherheitsimplikationen durch Cloud-Anbieter und -Standort

OmniCloud
Sichere Nutzung von Cloud-Speicher

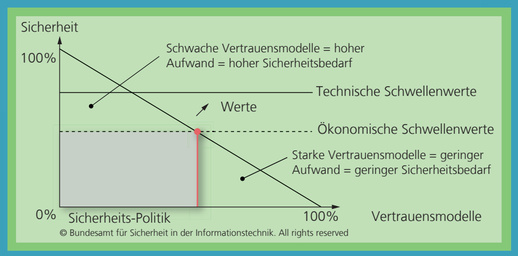


DIE IT-SICHERHEITSLEITLINIE SOLLTE KURZ UND ÜBERSICHTLICH SEIN!

Sie soll die folgenden Punkte enthalten:
1. Der Stellenwert der IT-Sicherheit und die Bedeutung der IT für die Institution müssen dargestellt werden.
2. Die IT-Sicherheitsziele und der Bezug der IT-Sicherheitsziele zu den Geschäftszielen und Aufgaben der Institution müssen erläutert werden.
3. Die Kernelemente der IT-Sicherheitsstrategie sollten genannt werden.
4. Die Leitungsebene muss allen Mitarbeitern aufzeigen, dass die IT-Sicherheitsleitlinie von ihr getragen und durchgesetzt wird. Ebenso muss es Leitaussagen zur Erfolgskontrolle geben.
5. Die für die Umsetzung des IT-Sicherheitsprozesses etablierte Organisationsstruktur muss beschrieben werden.

SICHERHEITSBLOGS UND -NEWSLETTER

SANS-Newsletter: www.sans.org/newsletters
Bruce Schneier: www.schneier.com
Erich sieht: www.erichsieht.wordpress.com
Heise Security: www.heise.de/security



Fraunhofer SIT

Hauptsitz Darmstadt
Rheinstraße 75 · 64295 Darmstadt
Telefon +49 6151 869-339
Fax +49 6151 869-224
info@sit.fraunhofer.de

Standort St. Augustin
Schloss Birlinghoven · 53754 Sankt Augustin
Telefon +49 2241 14-3272
Fax +49 2241 14-3007
info-bi@sit.fraunhofer.de

www.sit.fraunhofer.de