

Forum 3: Krisenvorsorge

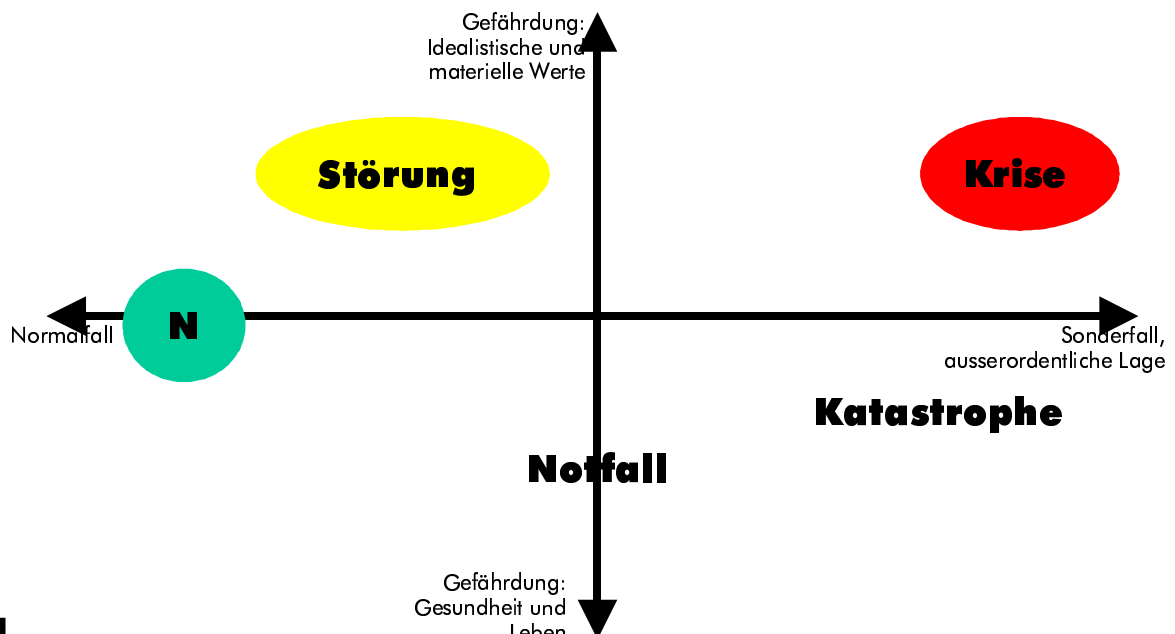
INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, LEADING SMALL PRINT IS IMPORTANT, ESPECIALLY IN A LEGAL CONTEXT.

Luzerner Forum für Informationssicherheit Verletzliche Informations-Infrastrukturen Forum 3: Die Krisenvorsorge in KMU

Marcus Holthaus	IMSEC	Cham
Stephanie Teufel	IIMT	Fribourg
Thomas Schlienger	IIMT	Fribourg
Adolf Flühli	ADF Consulting	
Jörg Klemm	n-able	Zürich
Roland Lörtscher	In&Out	Zürich
Jörg Schanze	IBM	Zürich

Begriffe

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, LEADING SMALL PRINT IS IMPORTANT, ESPECIALLY IN A LEGAL CONTEXT.



Fragestellungen

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, READING SMALL PRINT IS IMPORTANT, ESPECIALLY IN A LEGAL CONTEXT.

- Warum Krisenvorsorge
 - Totalausfälle vermeiden
 - Verpflichtungen einhalten trotz „widriger Umstände“
- Bandbreite der Krisen
 - Natur / Umwelt / Ressourcen
 - Aktionen Einzelner / Interner
 - Fremdeinwirkungen physisch / logisch
 - Presse / Medien
- Anforderungen an Krisenvorsorge
 - Schutz des Personals bei Krisen
 - Schutz der Unternehmung bei Krisen
 - „Weiterproduzieren“ trotz Ausfall externer Quellen
- Vorgehen
 - Identifikation schützenswerter Objekte
 - Identifikation der Abhängigkeiten
- Möglichkeiten der Krisenvorsorge
 - Redundante Maschinen, Systeme, Kommunikationsverbindungen
 - Personalpools, Picketts
 - Verteilung der Risiken auf Standorte / Systeme
- Unterschiede in der Krisenvorsorge von KMUs zu Grossunternehmen
 - Abhängigkeiten
 - Kosten
 - Angebote
- Angebote der Krisenvorsorge
 - Rechenzentren
 - Personalpools
 - Versicherungen
- Staatliche Unterstützung
- Konsequenzen bei fehlender Vorsorge

Spez. Probleme der KMUs

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, READING SMALL PRINT IS IMPORTANT, ESPECIALLY IN A LEGAL CONTEXT.

- Sensibilisierung fehlt
- Angst vor einem solchen grossen Projekt („Dampfwalzenansatz“):
 - > Schrittweise einer reifen Krisenvorsorge entgegengehen
- Unternehmer trägt u.U. mehr Risiken als Manager

Ansatz

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, LEADING SHALL PRINT & INFORMATION, ESPECIALLY IN A LEGAL CONTEXT.

- Make or Buy
- IBM BCRS Angebote (auch für KMUs)
 - Einmiete in ein RZ
 - Strategic outsourcing
- Ansatz: was wird wirklich gebraucht?
 - Je weniger vitale Geschäftsprozesse definiert, desto weniger Information wird auch benötigt.
 - Was kostet der Ausfall dieser Geschäftsprozesse?
 - Konzeptionelles Know-How fehlt bei KMUs, Geschäfts-Know-How ist gut
 - Ausgehend vom Worst Case Szenario müssen die Verantwortlichen die Kosten für den Ausfall der Geschäftsprozesse schätzen
 - IT und Business verschmelzen

Wie vorgehen?

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, LEADING SHALL PRINT & INFORMATION, ESPECIALLY IN A LEGAL CONTEXT.

- Entwicklung sinnvoller Business Continuity
 - Kennen der Prozesse
 - Verbände sind gefordert
 - Serviceleistung
 - Kontakte
 - IT-Dienstleister
- Einfache und klare Konzepte
 - Komplexität sollte entsprechend Umfeld sein

Risikoklassen mit Krisenpotential

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER QUOTE POTENTIAL THAN TECHNOLOGY, LEADING SHALL PRINT & INFORMANT, ESPECIALLY IN A LEGAL CONTEXT.

- Menschliches Versagen (unbewusst oder unbewusst)
- Wasser, Feuer
- Einbruch
- Ausfall von Kommunikationseinrichtungen
- Viren
- Datenmanipulation, -verlust
- Wissen der Mitarbeiter
- Verletzung von Gesetzen
- Vandalismus
- Hardware-Defekte (ICT)

Typische Risiken für KMUs

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER QUOTE POTENTIAL THAN TECHNOLOGY, LEADING SHALL PRINT & INFORMANT, ESPECIALLY IN A LEGAL CONTEXT.

- Wissen ist in wenigen Köpfen
-> Loslösung von einzelnen Personen, hin zu Prozessen
- Viele single-points of failure

Lösungen

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, LEADING SHALL FEEL & INFORMANT, ESPECIALLY IN A LEGAL CONTEXT.

- Sharing zwischen KMU-Informatikverantwortlichen/-Ressourcen?
 - Z.B. AS/400 1:8 im IBM-RZ
 - Ressourcensharing durch Branchen-Verbände?

Kosten der Krisenvorsorge

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, LEADING SHALL FEEL & INFORMANT, ESPECIALLY IN A LEGAL CONTEXT.

- Braucht eine Business Impact Analyse
- Darf nicht teurer werden als der laufende Betrieb
- Gleichzeitig produktive Nutzung
- Braucht zus. Spezialisten (kann outgesourct werden)

- Zusatznutzen: deckt organisatorische und technische Mängel auf

Information Assurance für KMUs

INFORMATION SECURITY IS A PROCESS AND A GOAL, NOT A STATE. SECURITY ENGINEERING IS ABOUT MAKING SURE THINGS DON'T NOT WORK, SECURITY IS ONLY AS STRONG AS THE WEAKEST LINK, SO DO NOT FALL FOR FALSE PROMISES BY SECURITY VENDORS, HUMANS HAVE A FAR GREATER SECURITY POTENTIAL THAN TECHNOLOGY, LEADING SMALL FIRM & IMPORTANT, ESPECIALLY IN A LEGAL CONTEXT.

- Sonia/Melanie sind auf einer hohen strat. Ebene
- Daher teilw. für KMUs zu theoretisch
- IA trägt aber für die Sensibilisierung der KMUs bei, dennoch weiter Awareness-Förderung notwendig
- KMUs brauchen eine nationale „CERT“/Notfallzentrale, an die sie sich wenden können