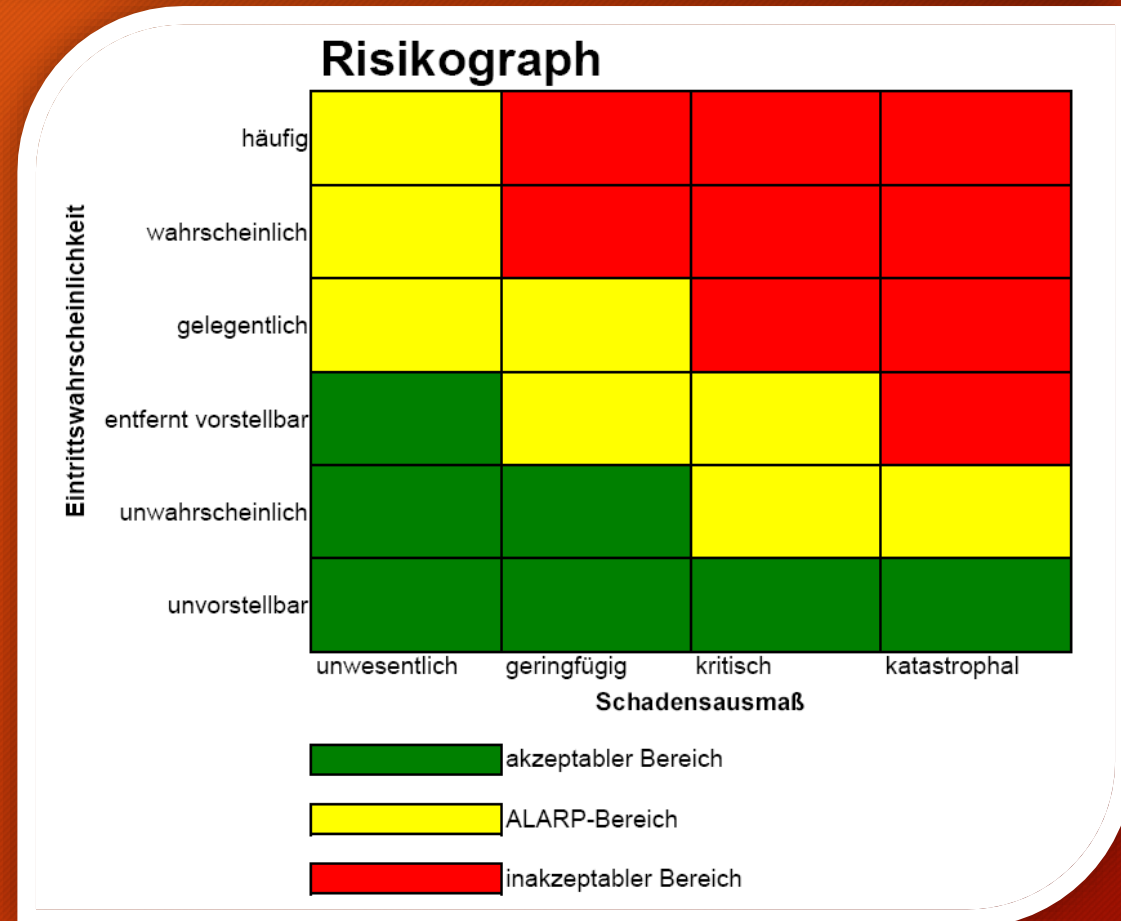


FireWall Möglichkeiten und Grenzen

CIT Ebikon
Consulting
State of the Art Security

Risk of Threats

Ermittlung des Risikos
anhand einer Risikoanalyse
und Feststellung des
Schutzbedarfs



Was ist überhaupt eine FireWall?

- Ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
- Ein Teil eines Sicherheitskonzeptes
- Eines der ersten Massnahmen, um die Verbindung intern zum Internet zu schützen
- Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden.

Sicherheitsziele bei der Umsetzung eines umfassenden FireWall Systems

- Alle Unsicherheiten mit grösstmöglicher Wahrscheinlichkeit vollständig eliminieren
- Möglichst viele Unsicherheiten mit passenden Sicherheitsmechanismen entgegen wirken, damit die Wahrscheinlichkeit eines Schadens auf eine praktisch nicht vorkommende Grösse minimiert wird
- Unsicherheiten, die nicht verhindert werden können, zu erkennen, um im Angriffsfall angemessen zu reagieren
- Angriffe im Vorfeld erkennen, damit erst gar kein Schaden entstehen kann

Schutzmassnahme FireWall von extern

- Gesicherte Verbindungen (VPN) Tunnel über Internet aufbauen (Standort Verbindungen)
- Externe VPN Verbindungen in die Praxis aufbauen Road Warrior
- Externe Angriffe abwehren, die mithilfe von technischen Mitteln vonstatten gehen (ungewollte Zugriffe)
 - DDos Attacken abwehren
 - Schädlichen Datenstrom analysieren und abwehren
 - Angriffe auf Dienste und Ports abwehren
 - Schädliche Scan Attacken abwehren (Informationsunterbindung)
 - Abwehr von Trojanern, Ransomware, Würmer etc. / innerhalb des Möglichen einer Firewall
 - Analysieren von Quelltexten auf Schadhafte Inhalte (Phishing Seiten, Werbebanner)

Schutzmassnahmen FireWall intern

- Unterbinden von Zugriffen zum Internet (Contentfilter)
- Proxy Server (Unsichtbarkeiten von Clients -> Internet)
- P2P Netzwerke verbieten (Bittorrent Clients zum Beispiel)
- GeoIP Blockierungen
- Zugriffsteuerungen in Zeiten und IP basierend
- Quality of Services (in Zusammenhang mit VoIP)
- Monitoring (Überwachung) des Netzes
- Ausgefeilte LOG Auswertungen (was passiert im Netz)

Welche Arten von FireWall gibt es?

- Externe Hardware FireWall (Schutz einer ganzen Infrastruktur, technisch)
- Software FireWall (Schutz eines einzelnen PC (meist nur Portbasierend und für Dienste)
- Web Applikation FireWall (WAF) (Schutz eines Web Servers)
- Proxy FireWall (Nutzdaten Analyse, einzeln oder als Teil einer Hardware FireWall)
- Paket Filter FireWall

Filtertechnologien FireWall (Hauptaufgaben)

- Paketfilter (Grundfunktion aller FireWall Technologien)
- Stateful Inspection (erweiterte Form der Paketfilterung)
- Proxyfilter (Stellvertretende Anfragen zum und vom Internet / Unsichtbarkeit)
- Contentfilter (Blockieren und Sperren von unerwünschten Inhalten)
- Deep Packet Inspection (Data Loss Prevention / Verschlüsselte Daten analysieren)
- FireWall Regelwerke (Rule Sets / IPTables)

Wie sicher ist eine FireWall (High-Level)

- Ziele

- analysiert, kontrolliert und reglementiert die Kommunikation entsprechend einer Sicherheitspolitik / Sicherheitsrichtlinien
- protokolliert sicherheitsrelevante Ereignisse
- alarmiert bei erheblichen Verstößen (Log Auswertung)
- Vertraulichkeit wahren
- Verhinderung einer gezielten Manipulation von Daten
- Missbrauchererkennung
- Erkennung von Anomalien
- Protokollierung und Berichtserstattung
- Verschlüsselung von Daten zwischen 2 Standorten (Zum Beispiel mit IPSec)

Wo sind die Grenzen einer FireWall?

- Eine FireWall schützt grundsätzlich nicht vor böartigen Inhalten, die auf den zugelassenen Wegen in das lokale Netzwerk gelangen
- Die Auswirkungen einiger Viren und Würmer werden zwar unterbunden, weil die Kommunikation über die benötigten Ports gesperrt ist, aber einen echten Schutz vor Viren und Trojanern bietet die FireWall allein nicht
- Das Abhören von sensiblen Daten im Internet wird durch die FireWall nicht verhindert
- Vertrauliche Informationen wie Verträge, Passwörter, Entwicklungsinformationen etc. sollten daher auch bei Einsatz einer FireWall nur geschützt übertragen werden, z. B. durch den Einsatz geeigneter Verschlüsselungsverfahren oder über VPN-Verbindungen

FireWall im Informationssicherheitsmanagement (ISMS)

- Eine FireWall ist somit ein Teil der
 - Vertraulichkeit
 - Integrität
 - Verfügbarkeit
- Ohne FireWall darf heute keine Infrastruktur an das Internet angeschlossen werden

FireWall - Einer der wichtigsten Segmente der IT-Sicherheit

- Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken
- In der Praxis orientiert sich die Informationssicherheit im Rahmen des IT-Sicherheitsmanagements unter anderem an der internationalen ISO/IEC-2700x-Reihe.
- Im deutschsprachigen Raum ist ein Vorgehen nach IT-Grundschutz (BSI - Bundesamt für Sicherheit in der Informationstechnik) praktikabel, da Anlehnung an ISO / IEC 2700x

Motivation und Ziele der Informationssicherheit

- Information (oder Daten) sind schützenswerte Güter (Assets). Der Zugriff auf diese sollte beschränkt und kontrolliert sein. Nur autorisierte Benutzer oder Programme dürfen auf die Information zugreifen. Schutzziele werden zum Erreichen bzw. Einhalten der Informationssicherheit und damit zum Schutz der Daten vor beabsichtigten Angriffen von IT-Systemen definiert.
- **Allgemeine Schutzziele:** Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität

Partnerschaften



- Bundesamt für Sicherheit in der Informationstechnik (BSI)



- Information Security Society Switzerland

Git´s no öppis?



Bei Fragen rufen Sie uns an
079 267 40 41

Kontakt



IT-Consulting Ebikon - State of the Art Security

CEO Markus Opfer-Rodrigues

SSCP / CCSP / CISSP & Wirtschaftsinformatiker

D4 Business Village Luzern

Platz 3, 6039 Root D4

Mail: support@it-consulting-ebikon.ch

Telefon: 079 267 40 41

<https://IT-Consulting-Ebikon.ch>

<https://Adele-FireWall.swiss>

<https://shop.Adele-FireWall.swiss>

<https://Selena-Server.swiss>

<https://Levar.ch>

Wir halten das, was wir versprechen

[Download Firmenbroschüre](#)

[Download Code of Ethics](#)

Oder unter <https://IT-Consulting-Ebikon.ch> - Über ITCE