Was soll den groß passieren?:
Vermutungen und Hoffnungen von Laien

Bei mir ist nichts zu holen!:
Gedanken zu Bedrohungsszenarien

Typologie von Angreifern

Schutzwürdige Objekte

Abschätzung des Risikos, wirtschaftliche Bewertung

Ich kann ja doch nichts machen :(
Mögliche Maßnahmen

Die Hacker sind draußen

lt. FBI(1995) werden 85% aller Angriffe
mit Insiderwissen ausgeführt.

Mich trifft es nicht / Ich bin zu unbedeutend

Jeder am Internet angebundene Computer kann als
Rechner für eine Denial of Service Attacke dienen

Ich habe eine Firewall / Mein Provider macht das für mich

Der ist gut (Spam, Würmer, Viren, Relaying)

Meine Antivirensoftware schützt mich

Der ist sogar noch besser (Spionage-Webseiten,
Malicious Flash, Java Applets, Adware)

Bisher ist auch nichts passiert / Das ist nur Panikmache

Die meisten Attacken passieren unentdeckt
95% der Datensicherungen wurden nie getestet

Schau mal, wer da hämmert

Typologie von Angreifern

Skills	Fin./techn. Aufwand	Risiko	Zielsetzung
Keine	Kein Aufwand	Kein Risiko	Eindringen
Geringe	Wenig Aufwand	Geringes Risiko	Spionieren
Training	Technologie	Mittleres Risiko	Verändern
Spezialist	HiTech		
Expertenteam	Viel Aufwand	Hohes Risiko	Zerstören

Schau mal, wer da hämmert

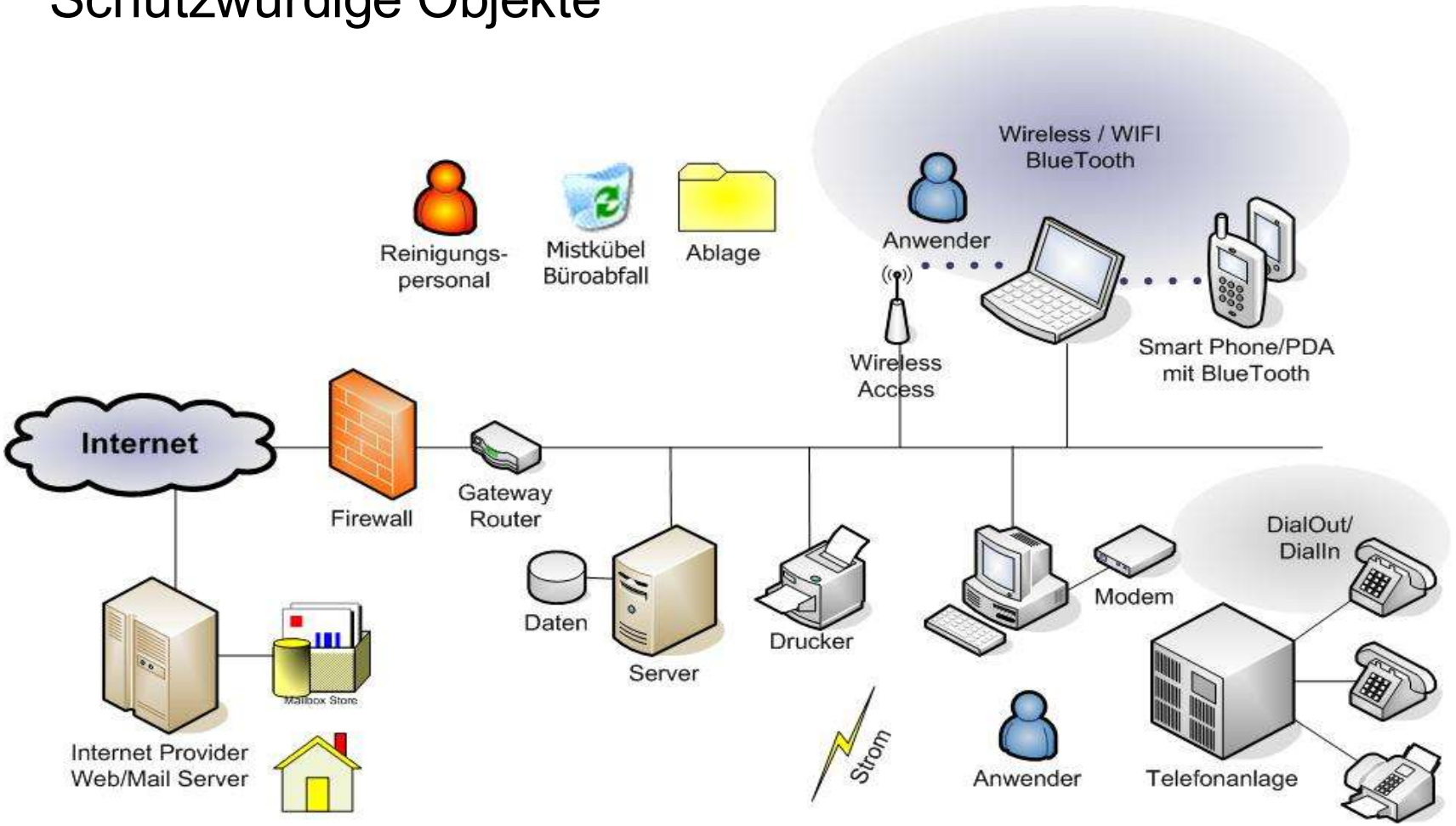
Typologie von Angreifern

Skills	Fin./techn. Aufwand	Risiko	Zielsetzung	Angreifer
Keine	Wenig Geld	Hohes Risiko	Zerstören	**Terrorist**
Geringe	Wenig Aufwand	Mittleres Risiko	Verändern	**Frustrierter MA**
Geringe	Wenig Aufwand	Geringes Risiko	Eindringen-Zerst.	**Skript Kiddy**
Spezialist	HiTech	Mittleres Risiko	Eindringen	**Hacker**
Spezialist	Technologie	Geringes Risiko	Spionieren	**Ind. Spionage**
Expertenteam	Viel Aufwand	Kein Risiko	Spionieren-Zerst.	**Government**
Expertenteam	Viel Aufwand	Mittl.-Hohes Risiko	Eindringen-Zerst.	**Militär**

Gegen Government und Militär gibt es keinen Schutz
(und gegen Nachlässigkeit auch nicht)

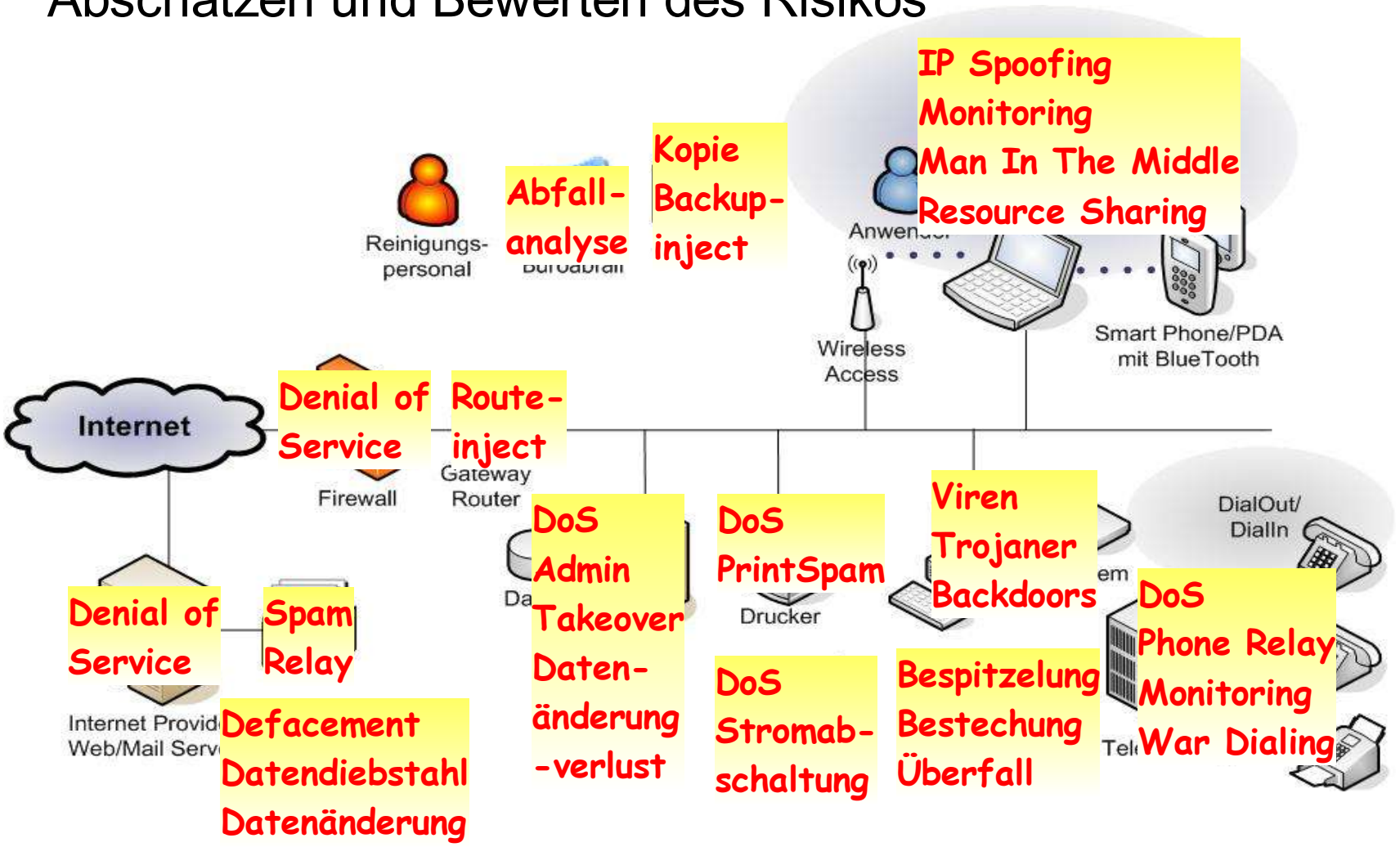
Wir haben einen Firewall...

Schutzwürdige Objekte



... und Antivirensoftware

Abschätzen und Bewerten des Risikos



Abschätzen und Bewerten des Risikos

Objekt	Potentielle Gefahr	Auswirkung
Fileserver	Datenveränderung, -verlust	Wiederherstellungskosten, Zeit-, Terminverlust
Webserver/Online Shop	Diebstahl von Kundendaten	Kreditkarten, Kundenabwerbung
	Preisänderungen	Umsatzeinbuße
Mail	Spam	Kosten für Bearbeitung von Mails
	Relay	Haftung bei Mitwirken an DoS-Attacken, Kommunikationsverlust bei relaygefilterten Domainen
Firewall	Denial of Service, Spoofing, Flooding,	Kosten für Bandbreite, Erstschutz gegen Aussen
Antiviren-SW	Zerstören oder Verändern von Daten	Nachvollziehbarkeit von Informationen, Kosten für Wiederherstellung
	Trojaner	Zugriff über Hintertüren auf die Systeme. Ausgangsbasis für weitere Angriffe
Modems (BuHa, eBanking)	Backdoors, Wardialer	Kommunikationskosten, Kritische Daten können ausspioniert werden, Haftungsfragen
Wireless	Mitlauschen, Spoofing	Spionage, Verlust von Wetbewerbsvorteilen, Haftung bei kritischen Transaktionen
Ablage, Archiv, Abfall	Spionage, Analyse von Abfällen, Korrekturausdrucken	Verlust von Wettbewerbsvorteilen, Regressgefahr bei geheimen Transaktionen

Erhöhen der Basisverfügbarkeit

Kleinstmögliche Installation,
stabile (aber aktuelle) Software,
Redundante Installation von Software
Sicherheitsupdates einspielen
Erstellen von Datensicherungen und externe Lagerung

Aufbau von Abwehrmaßnahmen

AV-Software auf Arbeitsplätzen und Servern aktualisieren
Abteilungen durch Router und Firewalls trennen
Personal Firewalls auf allen Arbeitsstationen und Servern
Eventlogs
Definieren von Zugriffsrechten, Sicherheitsrichtlinien und Verhaltensrichtlinien
Erzwingen komplexer Passworte und regelmässige Änderung

Aufbau von Früherkennung

Firewalls und AV-Software müssen Anomalien per Mail an einen Verantwortlichen melden
Abonement von Sicherheitsmeldungen der SW-Hersteller
Regelmässige Durchsicht der Eventlogs auf aussergewöhnliches Wachstum und Vorkommnisse

Aufbau eines konventionellen Notfallsystems

Konventionelle Ablage von Dokumenten
Verträge mit Lieferanten über Notsysteme
„Notfallsmappe“ mit aktuellen Ansprechpartnern und Telefonnummern
Ernennen eines Verantwortlichen „Kümmerers“

Erhöhter Widerstandes beim Eintritt von Fremden reduziert deren Erfolgschance und Interesse

Regelmässige Überwachung zeigt mögliche Angriffe auf

Früherkennung läßt Raum für Gegenmaßnahmen

Trainierte Notfalls- und Wiederanlaufszenarien reduzieren die Ausfallskosten

Regelmässige Anpassung an neue Szenarien gewährt wirksamen Schutz

Fragen?

w.rogner@rsb.at