



IT-Sicherheit (II)

oder besser
Informationssicherheit - Herzstück des Unternehmens



Kurzvorstellung des Referenten

Marcus Beyer (76)
Dipl. Kommunikationswirt

Inhaber von nextsolutions

Themen u.a.:
Sicherheitsberatung, Sicherheitskulturanalyse
und Security Awareness

Chefredakteur des Online-Fachportals
Securitymanager.de

www.nextsolutions.de
www.securitymanager.de





Linktipp www.securitymanager.de

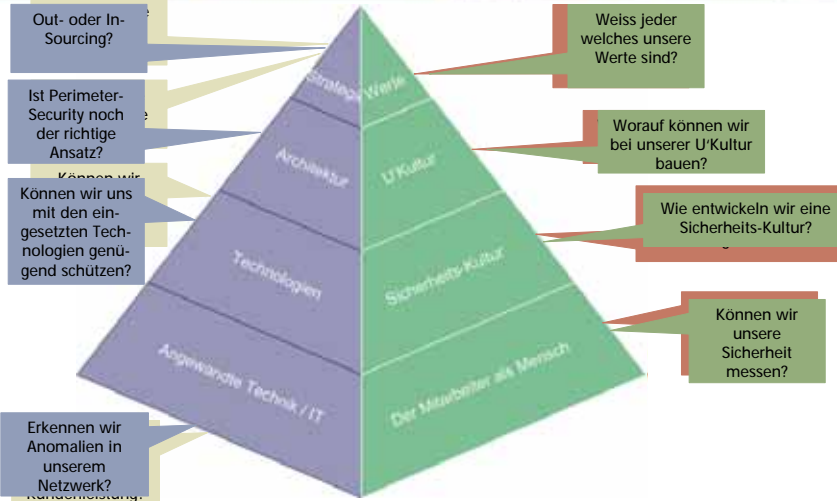


Agenda für den heutigen Abend

- Der ganzheitliche Blick auf die IT-Sicherheit
- Was uns Statistiken sagen
- Bedrohungsszenarien und die Trends in der IT-Security
- Wie kann ich mich effektiv schützen, worauf muss ich achten – der Kurz-Check
- Ausblick und Empfehlungen



Ganzheitlicher Blick ist Voraussetzung



5



BSI-Studie: Die Lage der IT-Sicherheit in Deutschland 2005

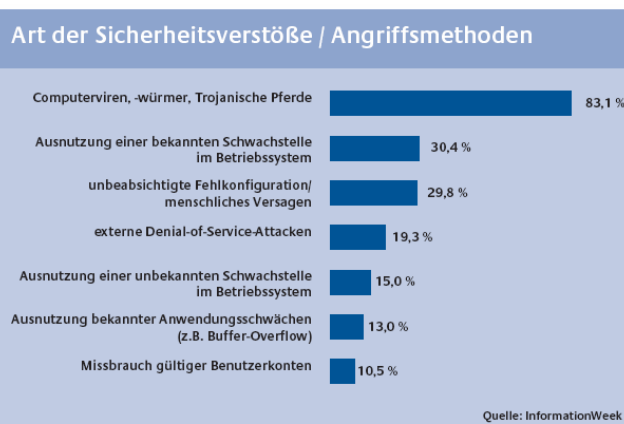


Abbildung 3: Verbreitung von Angriffsmethoden in deutschen und schweizerischen Unternehmen [8]

6



<kes>/Microsoft-Sicherheitsstudie 2006

Gefahrenbereich	Bedeutung		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,52	2	1,17	1	49 %
Malware (Viren, Würmer, Troj. Pferde,...)	2	1,06	1	1,51	4	35 %
Software-Mängel-/Defekte	3	0,60	5	0,58	2	46 %
Hardware-Mängel-/Defekte	4	0,55	6	0,34	3	45 %
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	5	0,50	3	0,63	7	12 %
unbeabsichtigte Fehler von Externen	6	0,39	7	0,32	5	30 %
Hacking (Vandalismus, Probing, Missbrauch,...)	7	0,37	4	0,59	8	12 %
Mängel der Dokumentation	8	0,27	9	0,27	6	20 %
Manipulation zum Zweck der Bereicherung	9	0,26	8	0,29	10	11 %
höhere Gewalt (Feuer, Wasser,...)	10	0,21	11	0,03	9	12 %
Sabotage (inkl. DoS)	11	0,17	10	0,22	11	10 %
Sonstiges	12	0,02	12	0,00	12	3 %

7



<kes>/Microsoft-Sicherheitsstudie 2006

Bei der Verbesserung der Informations-Sicherheit behindern am meisten ... (Mehrfachnennungen möglich, Auszug)	genannt von
Es fehlt an Geld	55 %
Es fehlt an Bewusstsein bei den Mitarbeitern	52 %
Es fehlt an Bewusstsein und Unterstützung im Top-Management	45 %
Es fehlt an Bewusstsein beim mittleren Management	37 %
Es fehlen verfügbare und kompetente Mitarbeiter	32 %
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	31 %
Es fehlen die strategischen Grundlagen / Gesamt-Konzepte	29 %
Die Kontrolle auf Einhaltung ist unzureichend	27 %
Anwendungen sind nicht für ISi-Maßnahmen vorbereitet	25 %
⋮	⋮
keine Hindernisse	3 %

8



Die IT-Sicherheit ist gefährdet durch...

- **Höhere Gewalt:** Feuer, Wasser, Blitzschlag, Krankheit, ...
- **Organisatorische Mängel:** Fehlende oder unklare Regelungen, fehlende Konzepte, ...
- **Menschliche Fehlhandlungen:** "Die größte Sicherheitslücke sitzt oft vor der Tastatur"
- **Technisches Versagen:** Systemabsturz, Plattencrash, ...
- **Vorsätzliche Handlungen:** Hacker, Viren, Trojaner, ...

9



Schadensbilanz:

- **Anzahl** der Sicherheitsvorfälle steigt stetig:
 - 75 % aller Unternehmen hatten im letzten Jahr Vorfälle mit geschäftsschädigenden Auswirkungen.
- **Schadenshöhe** eines Einzelschadens:
 - Maximum: hohe zweistellige Mio-Beträge
 - Durchschnitt: 5-6-stellige Beträge
- **Art der Schäden:**
 - größtes Einzelproblem: Computerviren
 - überwiegend ist der Grundwert Verfügbarkeit betroffen.
 - Überwiegende Mehrheit aller Vorfälle ist kein gezielter Angriff.
 - Rangfolge der Ursachen: Mensch, Technik, Umwelt

10



Klassische Aussagen

... Ich habe keine sensiblen Daten für die es sich lohnt in unser System einzudringen !

jedoch...

... Daten von Wettbewerbern sind immer von Interesse, oder?

....und: Das Management kann bei Umsatzverlusten, Insolvenzen usw. Aufgrund von IT-Ausfällen rechtlich belangt werden !!!

11



Die Realität?



12



Die Realität?

Offen wie Scheunentore

Klein- und mittelständliche Unternehmen stellen ihre Geschäftstätigkeit immer stärker auf das Internet, für viele aber ist davon, dass sie die auch durch diebstahlartige Gefahren stärker betroffen sind.



Zehn Prozent der KMU's in Deutschland ergreifen keinerlei Sicherheitsmaßnahmen für ihr Unternehmen.

Wozu Sicherheit, ich hab doch eine Firewall?!?



Was gilt es in unserem Unternehmen zu schützen?

- **Infrastruktur:**
Gebäude, Einrichtung und Hardware
- **Betriebsverfahren:**
Verfügbarkeit der EDV-Systeme, Verfügbarkeit und Integrität der Daten
- **Informationen:**
Angebote, Verträge, Inhalte von Verhandlungen, Daten über Verkaufsverfahren, Personaldaten, Personenbezogene Daten

Nicht zu vergessen: Das Ansehen Ihres Unternehmens in der Öffentlichkeit.



Woher kommen die Gefahren heute, woher morgen?

• Gefahren heute:

- DOS/DDOS
- Spam
- Malware
- Social Engineering
- (Wirtschafts-) Spionage

© Tages-Anzeiger; 10.06.2006; Seite 17

Zürich

REGION

Hacker gefasst

Zürich/Schwyz - Ein im Kanton Zürich wohnhafter **Hacker** hat über Pfingsten die Webseite seiner Wohngemeinde angegriffen. Die betroffene Homepage wird von einer IT-Firma im Kanton Schwyz betreut. Wie der Schwyzer Verhörer Georg Boller sagt, ist der 19-jährige Serbe geständig. Ein eigentliches Motiv sei nicht erkennbar. Der Mann habe aus «Gwunder» gehandelt. Der **Hacker** ist nicht in die Datenbank der Gemeinde eingedrungen. Durch den Angriff wurden auch andere Webseiten vorübergehend lahm gelegt. Die Firma hat eine Anzeige wegen Datenbeschädigung eingereicht. (hoh)

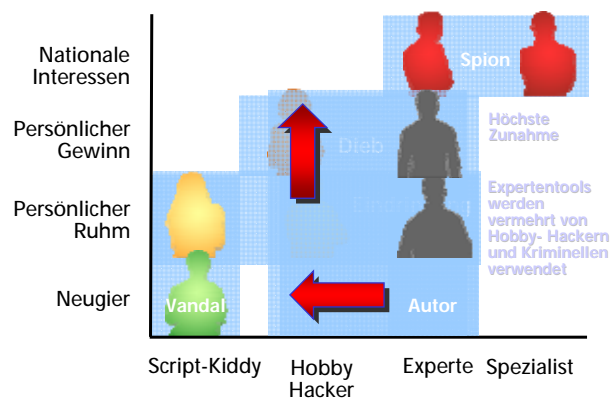
• Gefahren morgen:

- Siehe oben...

15



Woher kommen die Gefahren heute, woher morgen? – Die Akteure



Quelle: fedpol, MELANI / Cybercrime, Marc Henauer

16



Das Ganze in Zahlen

80% der Angriffe erfolgen von innen

- Fehler von Mitarbeitern (unwissend und/oder böswillig)
- neugierige Mitarbeiter
- Industriespionage

20% der Angriffe erfolgen von außen

- 19% der Angriffe sind DoS-Attacks oder Website-Hacks
- 1% der Angriffe beschädigen Firmendaten

17



Das Ganze in Zahlen

Schäden mit mittlerer und größerer Bedeutung:

- 8% Sabotage (inkl. DoS) und höhere Gewalt
- 9% Informationsdiebstahl/unbefugte Kenntnisnahme
- 38% Hardware-Mängel/-Defekte
- 43% Software-Mängel/-Defekte
- **51% Mitarbeiter-Irrtum und -Nachlässigkeit**
- **54% Malware (Viren, Würmer, Trojanische Pferde etc.)**

• Quelle: KES-Studie 2004

18



Der Autor heute!

- Befasst sich mit einer Vielzahl von Tätigkeiten, wie das Schreiben von Malware, Betreiben von Bot-Netzen, Durchführung gezielter Angriffe
- Hohes technisches Know-How – Ist ein „early adopter“, der vor allem individualisierte Malware einsetzt und mit Vorliebe noch nicht bekannte Sicherheitslücken ausnutzt.
- Verbindendes Element ist dabei die klare finanzielle Absicht.
- Gut organisiert und vernetzt, beschafft über und beliefert den Markt.

© Tages-Anzeiger, 15.03.2006, Seite 12

Kurzzeile

Zugang zu Bankkonten ergaunert

Zum ersten Mal haben Hacker in den USA Passwörter zu Bankkonten geknackt. Ermittler sprechen von einem der größten Datendiebstähle.

Von Walter Meederberger, New York

US-Banken mussten in den letzten Jahren zwar schon wiederholt Kreditkarten sperren und Millionenbeträge an bestohlene Kunden auszahlen. Doch zum ersten Mal haben Hacker nun geschafft, sich an Diebe nur trüben können, den direkten Zugriff auf die Bankkonten selber.

Nach monatelangen Ermittlungen bestätigte die Staatsanwaltschaft in New Jersey gestern, dass sie einem internationalen Beteiligungs auf die Schwäche gekommen sei und 14 Hacker verhaftet habe. Die Diebe sollen nicht nur in den USA, sondern auch in Grossbritannien, Pakistan, Rumänien und Spanien Konten gehackt haben. Über das Ausmass der Schadenssumme lagen zunächst keine klaren Angaben vor: «Die Diebe haben auch den Schlüssel gestohlen, der zur Entzifferung der PIN-Codes erforderlich ist», heisst es auf dem Sicherheits-Experten der Technologiefirma Gartner, mit die gelangt nach eigenen Angaben durch verschiedene Hinweise von Ermittlungsbehörden zum Schluss, dass es sich um den «schlimmsten Kartenmissbrauch aller Zeiten» handeln könnte, bisweilen aber um den «grössten PIN-Code-Diebstahl».

19



Malware - Preise und Leistungen

- Um sich von der Konkurrenz abzuheben, bieten viele Kriminelle sogar Preisrabatte, Testversionen, spezielle Angebote oder "Jahresversionen" von Schädlingen an, die kostenfrei aktualisiert werden.
- **Glauben Sie das?**

20



Übersicht über Artikel, die auf Untergrundservern gehandelt werden:

- Kreditkarte (0,50 – 5\$)**
- Bankkonto (30 – 400\$)**
- E-Mail-Passwort (1 – 350\$)**
- Mailer (8 – 10\$)**
- E-Mail-Adressen (2 – 4\$/MB)**
- Proxy (0,50 – 3\$)**
- Komplette Identität (10 – 150\$)**
- SCAM-Versand (10\$/Woche)**
- Sozialversicherungsnummer (5 – 7\$)**
- Benutzerschnittstelle (2 – 10\$)**

(Quelle: Symantec Internet Security Threat Report XII)

21



Malware - Preise und Leistungen

- Miete für Server bei 10 Millionen zu versendende Spam-Mails = ca. 500 Dollar verlangt.
- DDoS-Attack für eine Stunde = 10 bis 20 Dollar
- 1 Million E-Mail Adressen = um die 100 Dollar.
- Der Preis für Malware-Baukästen variiert je nach angebotenen Service. Beispielsweise:
 - MPack, ein Tool, das nach Sicherheitslücken sucht und die entsprechenden Exploits installiert, ist 1.000 Dollar wert
 - Limbo, ein Tool zum Verwalten von Bots, wird für 500 Dollar angeboten, und
 - der Trojaner-Baukasten Pinch kostet pro entwickelten Trojaner 30 Dollar

22



Ein Beispiel

▼ Subject: I offer the DDOS attack service !
From: ddos@safe-mail.net <DDOS Service> 
Date: 3/3/05 10:54
Newsgroups: alt.2600.cardz

HI,

I offer the DDOS attack service, I offer estimate of expense on hour base. Free demonstration (10 minutes).
The price is based on the difficulty to pull down the target website, for the free demonstration or information please contact :

DDOS Service at : ddos@safe-mail.net

23



Wirtschaftsspionage

- Ist ein alter Hut, aber dank dem Einsatz von IKT-Mitteln äusserst effizient und kostengünstig.
- Kommt staatlich unterstützt vor allem aus dem nordostasiatischen Raum...
- ...und vom netten Nachbarn nebenan.
- Im Falle von Firmenspionage werden die technischen Hilfsmittel über den Markt beschafft und pfannenfertig installiert zu Händen von Drittpersonen.
- Im Vordergrund stehen gekonntes Social Engineering und das neuste, was der Exploit-Markt zu bieten hat.

24



Stand heute - Die schlechten Nachrichten:

- Immer noch zu viele nicht korrekt konfigurierte Systems und Applikationen (alle Plattformen)
- Immer noch mangelhafte Verteilung / Installation von Patches und Konfigurationsänderungen
- Immer noch Konzentration auf Perimeterschutz, zu wenig Schutz / Überwachung der Endsysteme
- Dem Faktor Mensch wird noch zu wenig Aufmerksamkeit geschenkt - Das letzte Glied in der Kette.
- Wachsender Aufwand bezüglich Schwachstellen und Aufwand für die Reparatur / Härtung

Mehrheit der Maßnahmen ist weiter reaktiv, d.h. man wartet auf ein „erstes Opfer“.

27



Erkenne Deinen Feind!

- **Man kann sich nicht vor etwas schützen, was man nicht kennt!**
 - Die Frage ist nicht, **ob**, sondern **wann** man angegriffen wird!
 - Die Gefahren heute sind Script-Kiddies statt Netzwerkexperten und Technik-Freaks!
 - Geografische Grenzen sind irrelevant, das Internet ist weltumspannend und der Gegner nur einen Mausklick entfernt

28



Maßnahmen: Ganzheitliche Sicherheit

Physische Sicherheit

Gebäude- und Zugangsschutz



IT-Sicherheit

State-of-the-Art
Security Produkte & Technologien
anwendungsspezifische
Konfiguration

Organisatorische Sicherheit

Security Policies, Prozesse
praxiserprobte Vorgehensweisen

29



Trends: Organisation der IT Sicherheit

- IT-Security wird vom "Verhinderer" zum Beitraggeber für den Risk Management Prozess
- Informationssicherheit als Enabler der Unternehmenskultur
- IT Security wird zu Informationssicherheit und in den OpRisk Prozess integriert
- Engere Zusammenarbeit mit Auditoren, Revisoren, Compliance Managern, Law etc.
- Nächste Generation von ITSecOfficers und Spezialisten am Markt

30



Trends: Technologie der IT-Sicherheit

- Gemischte Attacks (technisch, organisatorisch, sozial) mit rein kommerziellen Hintergrund
- Zusammenwirken (technisch und wirtschaftlich) von "Malware"-Komponenten (z.B. Suche nach gültigen email-Adressen durch einen Virus und Weiterverkauf an Spammer)
- Identitätsdiebstahl erlebt einen Boom (auch durch Web2.0-Technologie und -Nutzung)
- Schneller, höher, weiter ...
- **Aber auch: keine definitive Lösungen gegen Spam, Phishing & Co. - trotz MS Vista.**

31



Eine typische Bedrohung für kommende Jahre

- **Zero Day Attacks (ZDAs):**
- Keine/kaum Vorwarnzeit
- Ursache und Wirkung sind schlecht differenzierbar
- Gegenmaßnahmen müssen in "Echtzeit" - also proaktiv - wirksam werden
- Gegenmaßnahmen müssen auf "Unbekanntes" reagieren

- **Risiken von ZDAs:**
- Gefahr der Flächenwirkung zu Beginn der Attacke
- Hohes Schadenspotential zu Beginn, da der Angriff auf dem Überraschungsmoment basiert
- Panik-Reaktionen der Betroffenen (Trennung vom Netz) erschweren die Reaktion und Reparatur
- Gezielte ZDAs (Denial of Service, Informationsdiebstahl usw.) gegenüber "lohnenden" Zielen



32



Zukünftige Entwicklungen

- "More of the same": Menge = Komplexität
- "The Fast an the Furious": schnell & schädlich
- "I'll be back": Angriff als "Türöffner" für mehr
- "Die hard": Angreifer "wehren sich" gegen Maßnahmen

Wir müssen lernen, unter ständiger Bedrohung und Angriffen den "Normalbetrieb" zu erhalten.

33



Zusammenfassung Bedrohungslage

- Professionelle Wirtschaftsspionage an der Tagesordnung.
- Wirklich gefährliche Angriffe sind eine Kombination von Social Engineering und technischen Attacken.
- Sensibilisierung der Mitarbeiter auf Gefahren unabdingbar. Aber auch Werkzeuge und Hilfsmittel Sicherheit zu leben!

34



Gegenmaßnahmen - WISSEN

- **Wissen was man hat** ("real time" IT-Inventarisierung)
- **Wissen wo man steht** (Release-stand, Patch Level, SLAs)
- **Wissen, wer man ist** (Identity-Management) **und was man darf** (Policy Setting)
- **Wissen wer was macht** (Log-Management, IDS/IPS)
- **Wissen was läuft** (CERT-management, SecEvent-Management)
- **Wissen wer, wie und wann auf was reagiert** (Security Team, Incident- und Krisen-Management, Notfallplanung)
- **Wissen wie was passiert ist** (Forensik, Auditing, Reporting)

© Tages-Anzeiger, 22.08.2006, Seite 23

Wirtschaft

Phishing-Attacke auf Migrosbank

Zürich. - In breit gestreuten Mails sind am Montag Kundinnen und Kunden der Migrosbank aufgefordert worden, Passwort und ähnliche Sicherheitsmerkmale auf einer Internetseite bekannt zu geben. Die Mails enthielten das Logo der Bank und die dreiste Drohung, alle Migrosbank-Konten, für die man nicht innerhalb Tagesfrist die entsprechenden Angaben eintrage, würden gesperrt.

Als Sofortmassnahme auf diese so genannten Phishing-Mails stoppte die Bank den Zahlungsverkehr via Internet und schaltete die Bundeskriminalpolizei ein. Zusätzliche technische Sicherheitsmassnahmen würden abgelehrt. Auf die betrügerischen Mails sei nicht einzugehen, warnte die Migrosbank. Viel viele Kunden bereits Opfer des Phishing geworden sind, konnte die Bank vorerst nicht abschätzen, die eingetriggerte Hotline werde aber rege genutzt.

Phishing-Mails sind täuschend echt aussehende Mails im Namen eines Finanzinstituts mit der Absicht, Zugang zu Konten zu erschleichen. Bisher ist hier zu Lande vor allem Postfinance davon betroffen gewesen. (AP/TA)

35



Compliance: Gesetzliche Anforderungen

- KonTraG - Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
- HGB (Sorgfaltspflichten, GoB)
- BGB (Haftungsaspekte)
- GmbHG und AktG
- BetrVG
- Datenschutzgesetze
- UrhG - Urheberrechtsgesetz
- PHG – Produkthaftungsgesetz
- ...

36



Was kann ich nun selbst tun?

Informationssicherheit in meinem Unternehmen heisst:

- Physische Sicherheitsvorkehrungen treffen, wie Firewall, Virenschutz, Backup-Systeme, Diebstahlschutz etc.
- Organisatorische Sicherheitsmassnahmen erarbeiten, wie z.B. Notfallhandbuch, Sicherheitsschulungen, Sicherheitsrichtlinien, Kontrollen und Audits



Linktipp www.sicher-im-netz.de





IT-Sicherheits-Kurz-Check von Deutschland sicher im Netz

I Management der IT-Sicherheit

- Existiert in Ihrem Unternehmen eine übergreifende IT-Sicherheitspolitik / -strategie?
- Sind Ihre geschäftskritischen Informationen/Daten vollständig klassifiziert? Werden vertrauliche Informationen sicher übermittelt?
- Werden Sicherheitsvorfälle im Unternehmen analysiert? Sind Sie über den aktuellen Stand der IT-Sicherheit umfassend informiert? c c
- Haben Sie einen festen Ansprechpartner für Sicherheitsfragen benannt, der allen Mitarbeitern bekannt und für diese erreichbar ist?

39



IT-Sicherheits-Kurz-Check von Deutschland sicher im Netz

I Management der Informationssicherheit

- Etablieren Sie eine umfassende Sicherheitspolitik sowie ein Sicherheits-Management in Ihrem Unternehmen.
- Ihr Wissen um geschäftskritische Informationen ist die Basis für wirksame Sicherheitsmaßnahmen. Verschaffen
- Sie sich vollständige Klarheit über das schützenswerte Gut Ihres Unternehmens.
- Führen Sie eine detaillierte Analyse der IT-Sicherheit und -Risiken im Unternehmen durch.
- Benennen Sie ein Sicherheits-Management-Team mit klar definierten Rollen und Verantwortlichkeiten im
- Unternehmen und informieren Sie die Mitarbeiter darüber.

40



IT-Sicherheits-Kurz-Check von Deutschland sicher im Netz

II Technik

- Sichern Sie geschäftskritische Daten regelmäßig? Lagern Sie die Sicherungen aus? Werden Sicherungsmedien und Recovery-Prozeduren auf Funktionsfähigkeit überprüft?
- Nutzen Sie Anti-Virus Programme und werden diese regelmäßig aktualisiert?
- Werden sicherheitsrelevante Programmkorrekturen (Patches) auf allen Systemen tagesaktuell eingespielt?
- Sind Server bzw. Serverräume gegen Zugriff bzw. Zutritt von nicht autorisierten Personen ausreichend geschützt?

41



IT-Sicherheits-Kurz-Check von Deutschland sicher im Netz

II Technische Maßnahmen

- Etablieren Sie ein zuverlässiges Datensicherungssystem, das regelmäßig durch Testläufe überprüft wird.
- Erarbeiten Sie ein Viren-Schutz-Konzept und setzen Sie dieses auf allen PCs und Servern im Unternehmen in die Praxis um. Achten Sie auf fortlaufende Aktualität.
- Spielen Sie sicherheitsrelevante Patches schnellstens ein. Erarbeiten Sie für kritische Systeme
- Test- und Rückfallszenarien, um Ihren Betrieb möglichst nicht zu gefährden.
- IT-Betriebsräume müssen vor unbefugtem Zugriff geschützt werden. Der Zutritt z.B. zu Serverräumen sollte auf autorisierte Personen beschränkt sein.

42



IT-Sicherheits-Kurz-Check von Deutschland sicher im Netz

III Organisation

- Existieren betriebsinterne Richtlinien und Anweisungen für E-Mail und Internet-Nutzung oder den Umgang mit Passwörtern?
- Existieren betriebsinterne Richtlinien oder Anweisungen für den Betrieb der IT-Infrastruktur (Richtlinien für Administratoren bzw. externe Dienstleister)?
- Sind Ihre Mitarbeiter auf die Inhalte der Sicherheitsrichtlinie geschult?
- Existieren Notfallpläne für den Schadensfall (z.B. Verlust geschäftskritischer Daten, Virusbefall oder Brand)? Sind alle Mitarbeiter über richtiges Verhalten in Notfällen informiert?

43



IT-Sicherheits-Kurz-Check von Deutschland sicher im Netz

III Organisatorische Maßnahmen

- Eine firmenübergreifende Sicherheitsrichtlinie ist die Basis für ein korrektes Verhalten der Mitarbeiter. Existiert diese bereits, überprüfen Sie sie auf Aktualität und gesetzliche Konformität und passen Sie sie ggf. an.
- Verhaltensanweisungen für Mitarbeiter im IT-Betrieb (Administratoren, Entwickler, etc.) legen Sie idealerweise in einer weiteren, technisch detaillierteren Sicherheitsrichtlinie fest.
- Informieren Sie Ihre Mitarbeiter durch Schulungen /Trainings oder andere Sensibilisierungsmaßnahmen über die in der Sicherheitsrichtlinie festgeschriebenen Regelungen und Vorgaben.
- Notfallhandbücher sollten ebenso selbstverständlich sein wie Fluchtpläne. Informieren Sie Ihre Mitarbeiter über Inhalt und Aufbewahrungsort.

44



IT-Sicherheits-Kurz-Check von Deutschland sicher im Netz

IV Datenschutz

- Werden in Ihrem Unternehmen personenbezogene Daten verarbeitet?
- Sind mehr als vier Personen an der elektronischen Verarbeitung der personenbezogener Daten beteiligt?
- Hat Ihr Unternehmen einen Datenschutzbeauftragten bestellt?
- Werden die datenschutzrechtlichen Bestimmungen in Bezug auf Datenerhebung, -verarbeitung, -nutzung und -übermittlung eingehalten?

45



IT-Sicherheits-Kurz-Check von Deutschland sicher im Netz

IV Maßnahmen zum Datenschutz

- Die Verarbeitung persönlicher Daten unterliegt den gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes (BDSG).
- Sobald mehr als 4 Personen personenbezogene Daten in elektronischer Form verarbeiten, ist laut Gesetz ein Datenschutzbeauftragter zu bestellen.
- Eine pro forma- oder Nicht-Bestellung des Datenschutzbeauftragten kann erhebliche Geldbußen nach sich ziehen. Der DSB kann ein interner Mitarbeiter, aber auch ein externer Dienstleister sein.
- Durch Bestellung eines DSB und Schulung der Mitarbeiter vermeiden Sie Verstöße gegen das Datenschutzgesetz. Für evtl. Schäden aus der Verletzung datenrechtlicher Bestimmungen haftet das Unternehmen/der Geschäftsführer.

46



Linktipp www.bsi.de



Social Engineering

- Unerkanntes Eindringen in das Gebäude
- Anbringen eines Keyloggers an einem Arbeitsplatz
- Erfragen des Mitarbeiterpasswortes
- Entwenden eines PCs unter dem Vorwand der Reparatur
- Erfragen von Informationen zur Netzwerkkonfiguration durch Vortäuschung eines angeblichen Netzwerkproblems: („Gehen Sie ‚mal auf START – AUSFÜHREN – CMD und geben Sie mal IPCONFIG /ALL ein, was steht denn da alles?“)
- Versuch, sich eine/mehrere Dateien per eMail zusenden zu lassen, die beim Besuch auf einem Netzlaufwerk entdeckt wurde(n) und interessant erscheinen



Das schwächste Glied der Kette ...

Beispiele für Social Engineering

- Fall 1:
 - **Angreifer:** „Ihr Name lautet Johanna Schmidt?“
 - **Opfer:** „Ja.“
 - **Angreifer:** „Sie befinden sich im Nordflügel, fünftes Stockwerk, in der Buchhaltung?“
 - **Opfer:** „Ja.“
 - **Angreifer:** „Ihre Durchwahlnummer ist die 4365?“
 - **Opfer:** „Ja.“
 - **Angreifer:** „Ihr Benutzername lautet Jschmidt und Ihr Passwort ist ‚krokodil27‘?“
 - **Opfer:** „Nein, mein Passwort lautet ‚BugsBunny‘.“
- Fall 2:
 - **Angreifer:** „Guten Tag Herr Muster, ich habe in meinem Monitoring System einen massiven Outbreak eines Bots, der wohl von Ihrem System ausgeht und mir mein Quality of Service System nahezu aushebelt. Dadurch sind eine Menge Kollegen betroffen.“
 - **Opfer:** „Oh, das ist mir aber peinlich.“
 - **Angreifer:** „Wenn Sie mir Ihre Zugangsdaten geben, kann ich das vielleicht ohne großes Aufsehen remote debuggen.“
Etc.

49



10 Goldene Regeln für IT-Sicherheit

1. Den drei Gefahren ins Auge blicken

Grundsätzlich gibt es drei Gefahrenpotenziale:
Nicht-autorisierte Zugriff auf vertrauliche Daten von außen, Zugriff von innen durch unbefugte Mitarbeiter, Gefahren durch höhere Gewalt wie etwa Feuer.

2. Vor Fehlinvestitionen schützen

Bestandsaufnahme und Risikoanalyse

50



10 Goldene Regeln für IT-Sicherheit

3. Server sicher stellen

Server in einem zugangsberechtigten Raum aufstellen, Zugriffs- und Nutzungsrechte definieren.

4. Faktor Mensch berücksichtigen

Mitarbeiter müssen für Sicherheitsmaßnahmen sensibilisiert werden.

5. Abwehrmaßnahmen gegen Viren und Hacker treffen

Organisatorische und technische Maßnahmen, (Security Policy, Firewall, Anti-Virus-Software, etc.)

51



10 Goldene Regeln für IT-Sicherheit

6. Ungebetene Gäste nicht hereinlassen

Anti-Viren-Programme und Schulung der Mitarbeiter.

7. Den Schlüssel zur Sicherheit anwenden

e- Mails verschlüsseln

8. Den richtigen Partner finden

Ein starker Partner hilft, spezielle Sicherheitskonzepte zu erstellen, weiterzuentwickeln und zu optimieren.

52



10 Goldene Regeln für IT-Sicherheit

9. Die beste Wahl treffen

Die geeignetste Sicherheitslösung für das jeweilige Unternehmen auswählen, die ein Optimum an Sicherheit bietet.

10. Den schlimmsten Fall durchspielen und vermeiden

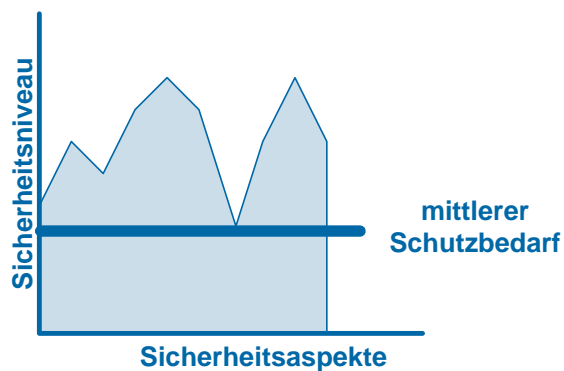
Im Falle eines totalen IT-Systemausfalls muss die Wiederherstellung der gesamten IT-Infrastruktur funktionieren - Diese Situation sollte regelmäßig im Unternehmen durchgespielt werden.

53



Erreichbares Sicherheitsniveau nach BSI-Grundschutzhandbuch

- schwieriges Thema aus der hohlen Hand heraus!
- erste Informationen unter www.bsi.de



54



Noch Fragen?

Kontakt:

nextsolutions
Marcus Beyer
Mobil: 0177 – 3228932
Mail: mb@nextsolutions.de



Sicherheit erfordert mehr als nur technische Maßnahmen...