Sicherheitsrisiken moderner Kommunikation

Gotha, 17.09.2012

Bernd König
CISSP und EDV-Sachverständiger im Ring Deutscher Gutachter

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP
ANSI
ISO/IEC 17024

Jeder technologische Wandel ist ein Teufelspakt,

bei dem der Nutzen und der Preis,
den man zahlen muss, nicht immer gleich groß sind.

Neil Postman, Kommunikationswissenschaftler

aus seiner Rede für die *Gesellschaft für Informatik am 11. Oktober 1990 in Stuttgart*

Agenda

- Begriffsbestimmungen
- Lage
- Bedrohungsszenarien
- Wer greift an / zu ?
- Wie geschieht es ?

Begriffsbestimmungen

- Cyberspace = Internet
- Cybercrime = Handtaschendiebe
- Cyberwarrior = Militärische Hacker

Bedrohungslage aus dem Cyberspace 2012

Nichts ist mehr wie früher:

Die Anforderungen an die IT- und Informationssicherheit haben sich extrem verschärft.

IT-Infrastrukturen werden meistens auf Netzwerk-Ebene durch Maßnahmen wie Firewalls, IPS/IDS und angemessene Segmentierung geschützt.

Es gibt Verschlüsselungsverfahren, mit denen die Vertraulichkeit geschützt werden kann

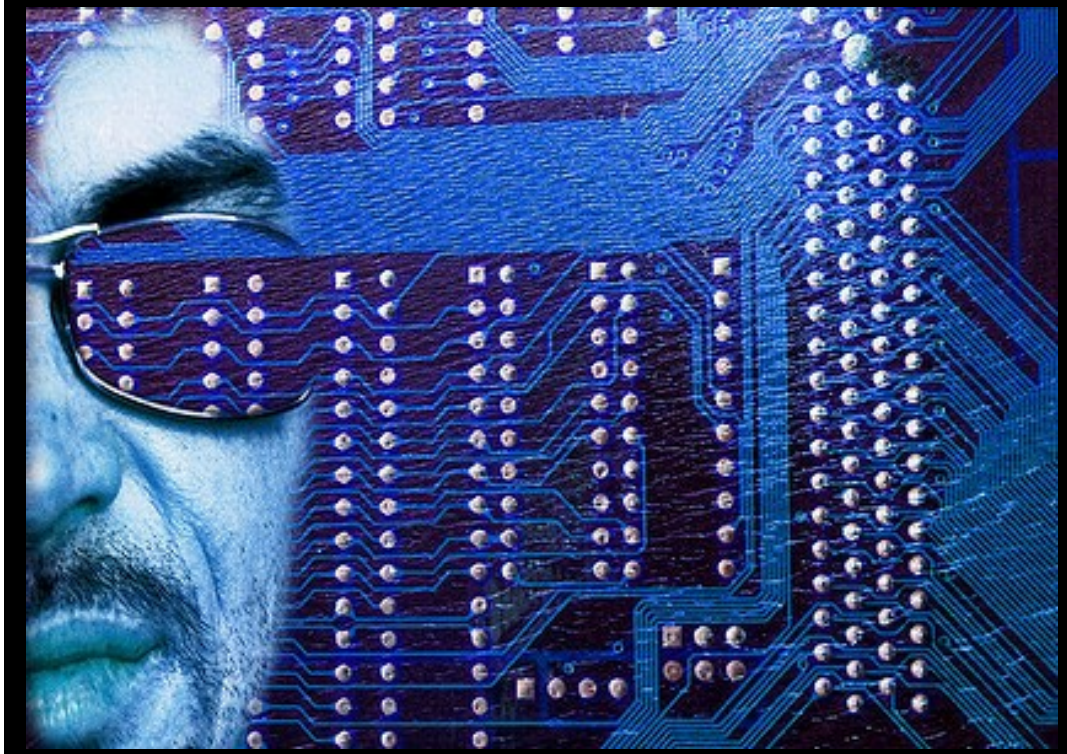
Doch Vorsicht:
Es kann trotzdem Sicherheitslücken geben,
die einen Angriff auf die Informationswerte ermöglichen.

Informationssicherheit

- Bedrohungsszenarien -

1	2	3	4
Angriff von Außen auf Plattformen im Internet	Eindringen von außen in interne Netze und Anwendungen	Info- Abfluss durch Innentäter, Geschäftspartner und Wettbewerber im internen Netz	Verlust von Daten und Infrastruktur

Mit wem haben wir es zu tun ?

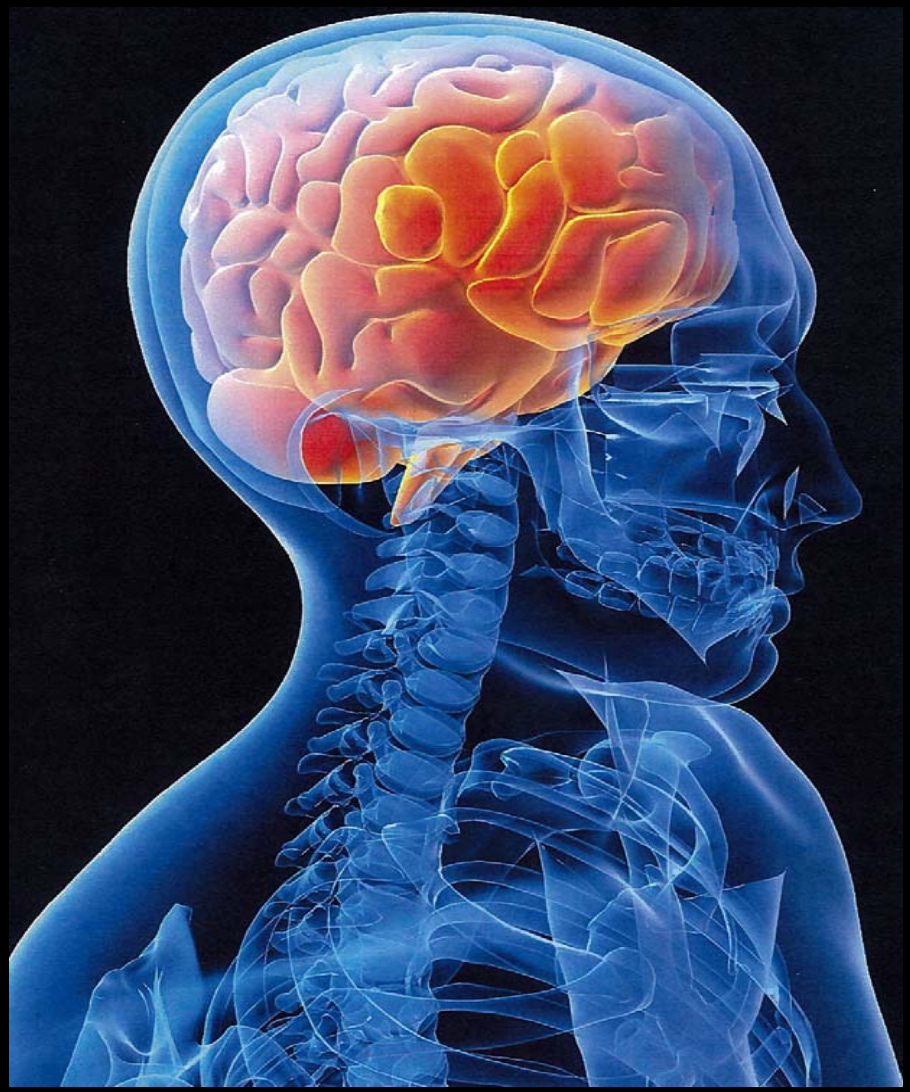


- Hacker
- Cyber-Kriminelle
- Cyber-Aktivisten
- Cyber-Terroristen
- Staatliche Nachrichtendienste
- Staatliche Cyber-Agressoren

Böser digitaler Werkzeugkasten

- Spionage | Trojaner
- Sabotage | Stuxnet
- Manipulation | Maninthemiddle
- Zerstörung | W32/ScarH
- Erpressung | Ransomware

Schwachstelle User



Was kann man tun ?

- IT-Sicherheitsstrategie
- Notfallmanagement
- Sichere Passwörter
- Datenverschlüsselung
- Zutritt, Zugang und Zugriff reglementieren UND kontrollieren
- Sinnvolle Restriktionen konsequent um- und durchsetzen
- Handlungskompetenz durch Information stärken
- Außergewöhnliche Maßnahmen zur Sensibilisierung
- Dynamisches Budget für Sicherheitsmaßnahmen

Patchen = Pflaster kleben

Patch Day

Microsoft adressiert 26+1 Sicherheitslücken

von Lars Bube

Share 0

14.06.2012

Zum aktuellen Patch Day hat Microsoft mit sieben Security Bulletins insgesamt 26 Sicherheitslücken in seiner Software geschlossen. Eine weitere kritische Lücke im XML-Befehlssatz muss allerdings von Hand beseitigt werden.

Keine Beiträge im Forum. » Diskussion starten!

Zum monatlichen Patch Day hat Microsoft am Dienstag wieder einige wichtige Updates für seine Software ausgerollt. Insgesamt gab es sieben Security Bulletins, die sich um 26 teils kritische Lücken drehten. Die Hälfte davon geht alleine auf den Browser Internet Explorer zurück, betroffen sind alle derzeit noch unterstützten Versionen vom IE6 bis hin zur Version 10 aus der Consumer Preview von Windows 8. Microsoft bezeichnete das MS12-037 deshalb als wichtigste Komponente der aktuellen Update-Runde und empfiehlt allen Anwendern und IT-Verantwortlichen den entsprechenden kumulativen Patch KB2699988 unbedingt umgehend zu installieren, sollte dies nicht automatisch erfolg sein. Die meisten der Lücken im Explorer waren im Frühjahr im Rahmen des Hacker-Wettbewerbs Pwn2own entdeckt worden. Einige davon hatten auch die Browser-Konkurrenten Google Chrome und Mozilla Firefox betroffen, die das Leck jedoch bereits innerhalb weniger Stunden nach seinem Bekanntwerden geschlossen hatten.

Quelle : crn.de

16:08 | **Umfassende Studie**

So gefährlich ist das beliebteste Passwort der Welt

Eine Studie der Universität Cambridge hat weltweit 70 Millionen Passwörter analysiert. Das am meisten verwendete ist so fantasielos wie fahrlässig – und öffnet Hackern Tür und Tor zu intimen Daten.

Von Elke Bodderas

© dpa

"123456", "password1" – Viele machen es Hackern mit zu einfachen Passwörtern allzu leicht

Ali Baba wusste das beste, berühmteste, unschlagbarste und wertvollste Passwort aller Zeiten und Erdteile: "Iftah ya simsim" – "Sesam öffne Dich". Drei Worte mit fantastischer Wirkung: knarzend, splitternd öffnete sich ein mächtiges Felsentor. Dahinter: alles, was sich ein Mensch erträumen kann.

Das Passwort aus Tausendundeiner Nacht hat inzwischen ein bisschen zugelegt, auf Hundertdreiundzwanzigtausendvierhundertsechsundfünfzig. In

WEITERFÜHRENDE LINKS

ARTIKEL

E-Mail

Kommen

MEISTGEL

Passwort

TOP 20 DER BELIEBTESTEN GEHACKTEN E-MAIL-PASSWÖRTER

1. 123456
2. 123456789
3. alejandra
4. 111111
5. alberto
6. tequiero
7. alejandro
8. 12345678
9. 1234567
10. estrella
11. iloveyou
12. daniel
13. 000000
14. roberto
15. 654321
16. bonita
17. sebastian
18. beatriz
19. mariposa
20. america

Quelle: www.acunetix.com

Wa$ 31n $1ch3r3$ Pa55w0r7 i$7

Wa$ 31n $1ch3r3$ Pa55w0r7 i$7

Breaking News …and Hashes

Über 6 Mio. Passwort-Hashes gestohlen

Passwörter zu LinkedIn Accounts gehacked

12.06.12 | Autor / Redakteur: Daniel Müller / Peter Schmitz

XING 0 Empfehlen Twittern 6 +1 0

PDF | Weiterempfehlen | Merken | Drucken

Mehrere Millionen Passwort-Hashes wurden aktuellen Informationen Zufolge aus dem Business-Netzwerk LinkedIn, sowie den Diensten eHarmony und Last.fm gestohlen. Inzwischen wurden wohl nahezu alle Hashes bereits entschlüsselt.

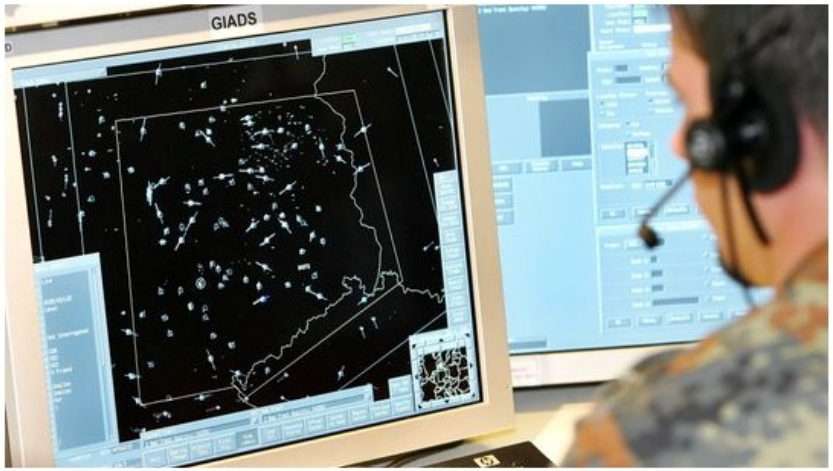
...Herausforderung Passwort(verwaltung)

- Für all diese Accounts und Schlüssel sind Kennwörter zur Authentifizierung notwendig.
- In der Regel führt die "Kennwort-Verwaltung" beim Nutzer fast zwangsläufig zu Sicherheitsrisiken.
- Die Nutzer beginnen in ihrer Not, Kennwörter zu notieren und zu hinterlegen, wodurch sie für Unberechtigte ggf. leicht zugänglich sind.

ELEKTRONISCHE AUFRÜSTUNG

Bundeswehr bereit für Cyberangriffe

Mit Viren Stromnetze lahmlegen, mit Würmern Atomanlagen zerstören: Die USA beherrschen den Cyberkrieg schon länger, die Bundeswehr hat nun offenbar nachgezogen.



Ein Bundeswehr-Soldat arbeitet an einem Computer in einem mobilen Gefechtsstand: So ähnlich könnten künftig auch Cyberattacken koordiniert werden.

Die Bundeswehr ist nach eigener Einschätzung zu Cyberangriffen auf Computer in der Lage. Die Streitkräfte hätten eine "Anfangsbefähigung" für Attacken in "gegnerischen Netzen" erreicht, heißt es in Unterlagen des Verteidigungsministeriums für den Bundestag, aus denen die *Financial Times Deutschland* (*FTD*) zitierte.

Demnach ist nach jahrelanger Vorbereitung eine neue Einheit für Computernetzwerkoperationen seit Ende 2011 einsatzfähig. Sie ist beim Kommando Strategische Aufklärung in Gelsdorf bei Bonn angesiedelt.

Fazit:

- Cyber War bedeutet Fortsetzung des Krieges mit anderen Mitteln auf einer anderen Ebene, dem Cyber Space, also dem Internet
- Jeder einzelne Nutzer im Internet ist somit ein potentielles Opfer
- Prävention besitzt also eine Schlüsselposition
- Die gestiegene Aufmerksamkeit muss mindestens auf diesem hohen Niveau gehalten werden

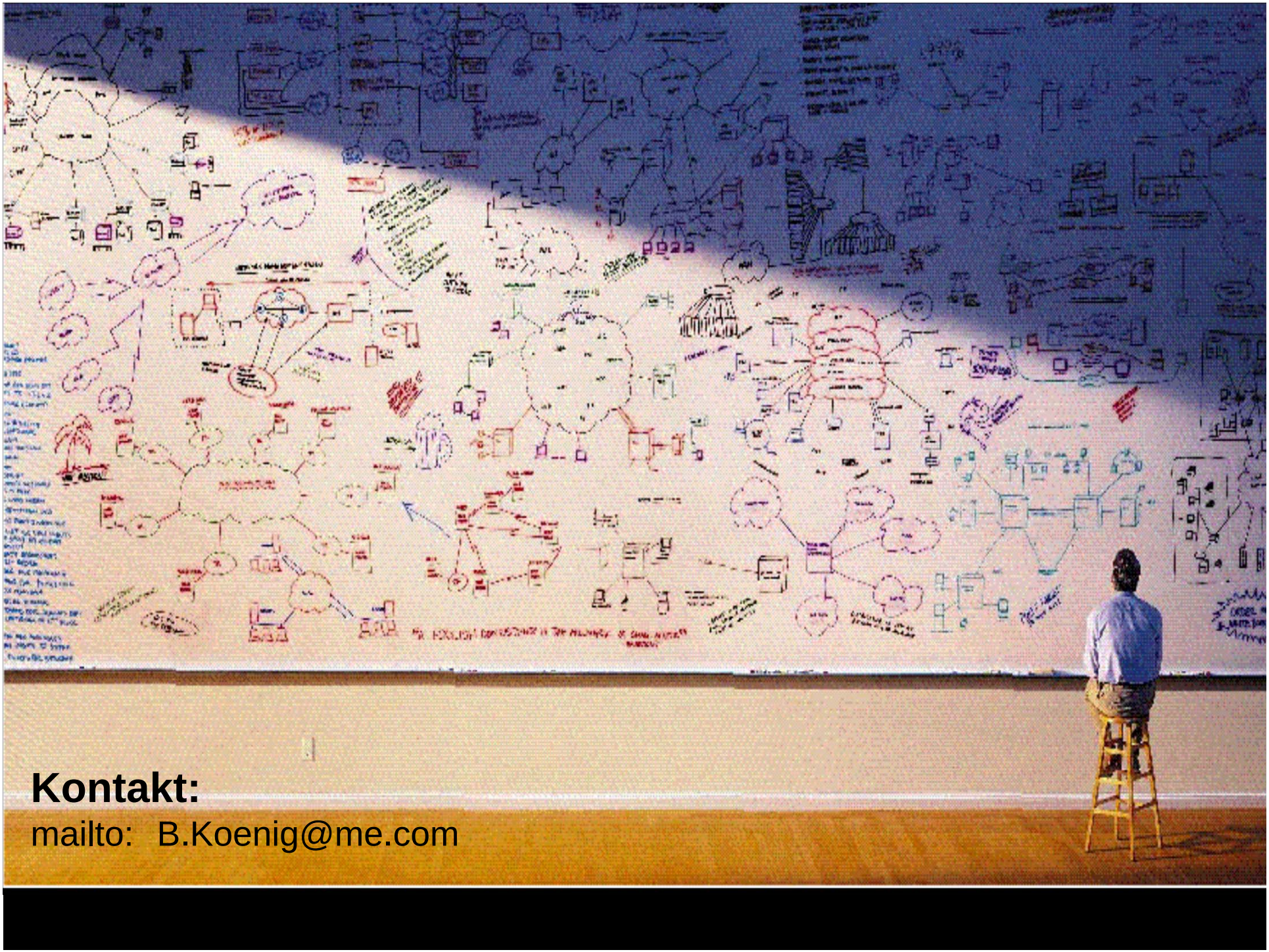
Wirksamer Schutz ?

Quelle : Tobias Hellsten / Piratenpartei

useful Links

- https://passwortcheck.datenschutz.ch/check.php
- https://shouldichangemypassword.com/
- https://www.microsoft.com/de-de/security/pc-security/password-checker.aspx
- https://www.sicher-im-netz.de/verbraucher/aktuelleGefahrenstufe.aspx
- https://www.buerger-cert.de
- https://www.botfrei.de/

Noch Fragen ?



Kontakt:
mailto: B.Koenig@me.com