Freie Universität Berlin

Blockkurs „Systemverwaltung”

Sommersemester 2008

IT-Security

Ingmar Camphausen – Rechnerbetrieb

Freie Universität Berlin

IT-Security in 2:30h

- **Ziele**
  - ⇒ Grundverständnis für Herangehensweise
  - ⇒ einige Sicherheitsbegriffe gehört haben
  - ⇒ Ideen, wo/wie man sich selbst bei Bedarf weiter informieren kann
  - ⇒ Erfahrungen aus der Praxis des Rechnerbetriebs vermitteln

Freie Universität Berlin

Struktur des Vortrags

- ☐ IT-Sicherheit – Ausgangssituation
- ☐ Grundlagen
- ☐ Der IT-Sicherheitsprozess an der FU
- ☐ Empfehlungen
- ☐ Informationsquellen
- ☐ Erfahrungen aus der Praxis des Rechnerbetriebs
- ☐ Ansprechpartner

Freie Universität Berlin

IT-Security – Ausgangssituation

☐ ... alles andere als rosig:

„Mean time to compromise < 5 min"

für ein ungepatchtes System, das ungeschützt online gebracht wird

Freie Universität Berlin

Problem der IT-Sicherheit

- ☐ Messbarkeit?
- ☐ gefühlt „nur Kostenfaktor“
- ☐ Durchsetzbarkeit von Eingriffen/ Sanktionen
  - ⇒ gegenüber Nutzern
  - ⇒ gegenüber Chefs
    - Verfügbarkeit/business continuity hat oft Vorrang vor Sicherheitserwägungen

Freie Universität Berlin

Problem der IT-Sicherheit (2)

- ☐ „typische“ Angriffe in ständigem Wandel:
  - Automatisierung
  - zunehmende Vernetzung
  - leistungsfähigere Netzanbindung

  ⇒ schnelle(re) Weiterverbreitung, kürzere Vorwarnzeiten
- ☐ immer weniger Knowhow für erfolgreiche Angriffe erforderlich:
  - „skript kiddies“, „Virus Construction Set“

Freie Universität Berlin

Problem der IT-Sicherheit (3)

- Trend zu „ubiquous computing“
  - ⇒ Beispiel Mobiltelefon/PDA: Zugriff
    - „jederzeit“
    - „von überall“
    - „auf alles“
- Besonders häufig durch Angehörige der Leitungsebene/„Entscheider“! :–}

Freie Universität Berlin

Situation wie die eines Torwarts?

- Eine kleine Unachtsamkeit entscheidet das Spiel zum Nachteil der eigenen Mannschaft...
- -zig Glanzparaden zählen dann nicht mehr...
- Aber: Die Situation ist nicht gar so hoffnungslos, denn...

Hoffnung (1)

- „St. Florians-Prinzip"
  - ⇒ „Oh heiliger Sankt Florian, verschon' mein Haus, zünd' andre an!"
    - » Es reicht häufig, etwas besser als andere (potentielle Ziele) geschützt zu sein (oder so zu wirken), so dass ein Angreifer es lieber dort versucht
- Schwächster Teil/schwächste Stelle bestimmt das Sicherheitsniveau des Gesamtsystems
  - ⇒ an der *richtigen Stelle* erreicht man durch Verbesserungen u.U. eine deutliche Erhöhung des Gesamt-Sicherheitsniveaus
  - ⇒ Es ist nicht sinnvoll, hohen Sicherheitsaufwand an ‚ungünstigeren' Stellen zu betreiben

Hoffnung (2)

- Wir fangen nicht bei null an!
- Rückgriff auf Vorarbeiten von anderen und auf existierende Ansätze
- Die meisten der gängigen IT-Sicherheitsmaßnahmen sind nicht geheim :-)

Freie Universität Berlin

Grundlagen

- ☐ Die 4 Schutzziele
- ☐ Kryptographie hilft!
- ☐ Rechtlicher Rahmen
- ☐ BSI-Grundschutz-Empfehlungen
- ☐ Zonen-Modell
- ☐ Risiko-Analyse
- ☐ Nutzer-Akzeptanz

Freie Universität Berlin

Schutzziele

- ☐ Die 4 „Grundpfeiler" der IT-Sicherheit
  - » bzw. negiert entsprechend die 4 Haupt-Bedrohungen

⇒ Vertraulichkeit
⇒ Integrität
⇒ Authentizität
⇒ Verfügbarkeit

» gelegentlich auch Nicht-Abstreitbarkeit...

Freie Universität Berlin

Kryptografie – oder: „Mathe hilft!“ ;-)

- Kryptografische Verfahren

  ⇒ helfen, mind. 3 der 4 Schutzziele zu erreichen:

  - Verschlüsselung (Vertraulichkeit)
  - Prüfsummen etc. (Integrität)
  - digitale Signaturen (Authentizität, ggf. auch Nicht-Abstreitbarkeit)

  ⇒ sind Grundlage für diverse Sicherheitsmechanismen

Freie Universität Berlin

Krypto – „Risiken und Nebenwirkungen“

- Gute Verfahren beziehen ihre Stärke aus der Konstruktion des Algorithmus und aus der Länge und Geheimhaltung der verwendeten kryptografischen Schlüssel, und *nicht* aus der Geheimhaltung des Verfahrens

  ⇒ Der Algorithmus kann offengelegt und von Fachleuten untersucht werden, ohne dass die Sicherheit des Verfahrens leidet

- Schlüsselmanagement...
- Fehler bei der Implementierung von eigentlich starken Krypto-Algorithmen
- Fortschritte in der Krypt-Analyse

Freie Universität Berlin

IT – kein rechtsfreier Raum (1)

- IT-Sicherheit, Vertraulichkeit:
  - ⇒ BVerfG-Urteil vom 27.02.2008 gegen Online-Durchsuchung:
    - „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"
  - ⇒ Fernmeldegeheimnis (Art. 10 GG)
  - ⇒ TKG, StGB (Computerkriminalität, §§ 202ff.)
  - ⇒ KontraG (Risikovorsorge als Aufgabe der Geschäftsleitung)
- Datenschutz:
  - ⇒ BDSG, Landesdatenschutzgesetze, Mediendienstestaatsvertrag

http://www.bverfg.de/pressemitteilungen/bvg08-022

Freie Universität Berlin

IT – kein rechtsfreier Raum (2)

- Mitbestimmung:
  - ⇒ PersVG
- Digitale Signaturen:
  - ⇒ SigG, SigV, Gesetz zur ‚elektronischen Form', VerwVerfÄndG, UStG
- Aufbewahrungsfristen:
  - ⇒ BGB, AO
- u.v.a.m. (unter anderem div. spezialgesetzliche Regelungen und Verordnungen)

Gesetz zur ‚elektronischen Form':

http://www.dud.de/dud/documents/formvorschriften-010

Freie Universität Berlin

Zonen-Modell

- Identifizieren von Bereichen mit vergleichbaren Sicherheitsanforderungen
  - ⇒ Gruppieren entsprechender Geräte etc.
- „innerste" Zone = höchstes Sicherheitsniveau
  - aber: was ist mit Angreifern „von innen"?!

Freie Universität Berlin

IT-Grundschutz

- Grundschutzmaßnahmen, Grundschutz-Kataloge des BSI:

  http://www.bsi.bund.de/gshb/index.htm

Freie Universität Berlin

Risikoanalyse

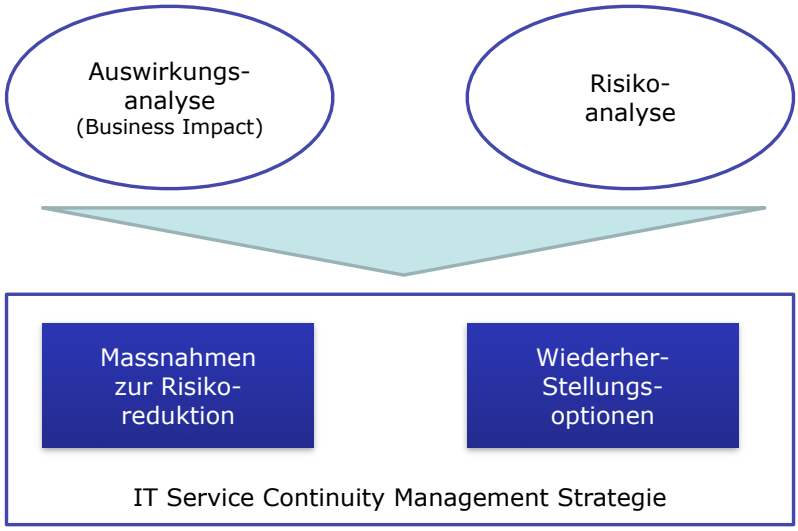
- Basis: Schutzbedarfsanalyse („worst case-Szenario")
  - ⇒ Abschätzung des möglichen/zu erwartenden Schadensumfangs *ohne Berücksichtigung von Schutzmaßnahmen*
- darauf aufbauend: Bedrohungs- und Risikoanalyse („wie häufig wird Schaden xy eintreten?" i.V.m. geschätzter Schadenshöhe)
- daraus abgeleitet: Maßnahmen zur Risikoreduzierung

19

Beispiel/ Vorgehensweise der an der FU Berlin gewählten Variante erläutert in der IT-Sich erh

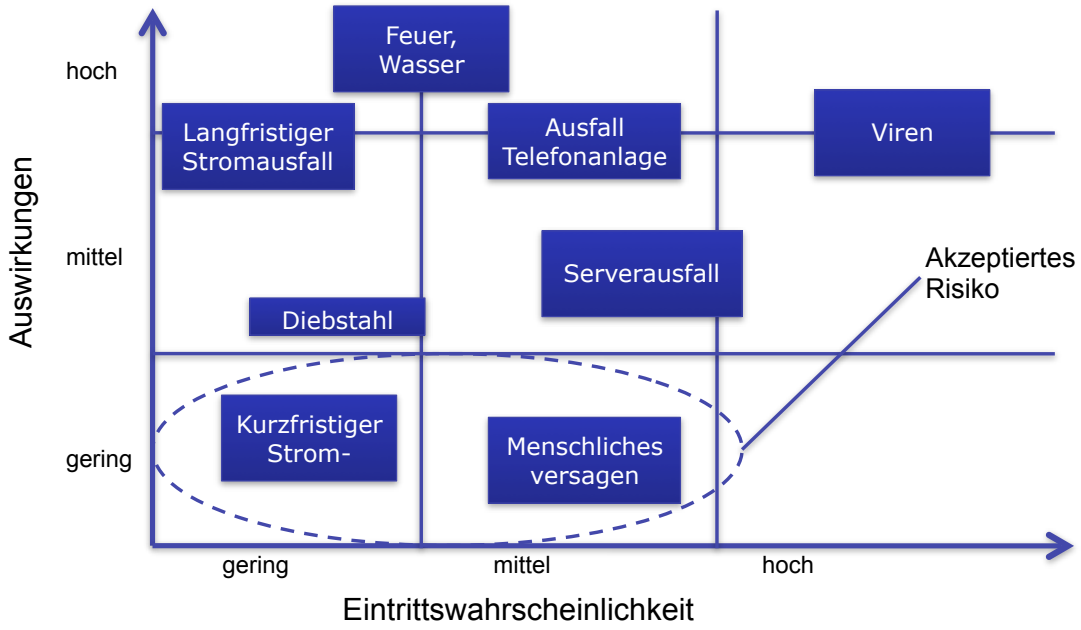
Freie Universität Berlin

Continuity Management



20

Continuity Management



Nutzerakzeptanz

- ☐ Sensibilisierung der Nutzer für IT-Sicherheitsfragen
  - ⇒ wichtig, weil sich manche Dinge rein technisch nicht verhindern lassen:
    - Öffnen von Mail-Anhängen/Downloads
    - Browser-Schwachstellen
      - z.B. sog. „zero-day exploits"
    - „Social Engineering"
- ☐ klare Regelungen zum sicheren Umgang mit IT
- ☐ konkrete Hinweise/Vorgaben
- ☐ Überschaubare Regelungen

Freie Universität Berlin

Der IT-Sicherheitsprozess an der FU

- Organisatorische Verankerung von Maßnahmen zur längerfristigen Gewährleistung der IT-Sicherheit:
  - ⇒ Etablierung von ausdrücklichen IT-Ansprechpartnern in allen FU-Bereichen und eines zentralen „Quasi-IT-Sicherheitsbeauftragten"
  - ⇒ Erfüllung der gesetzlichen Mitbestimmungsanforderungen
  - ⇒ Dokumentation aller IT-Verfahren an der FU (auch für Datenschutz [Verfahrensverzeichnis!])
  - ⇒ zentrale IT-Steuerung; IT-Überblick für FU-Leitung (u.a. durch Dokumentation!)
  - ⇒ IT-Sicherheitsrichtlinie (seit 2005, ab Sommer 2008 für gesamte FU)

Freie Universität Berlin

Die IT-Sicherheitsrichtlinie der FU

- Idee: Alle wichtigen Aspekte in einem **Zentraldokument**
- richtet sich sowohl an **IT-Personal** als auch reine **IT-Anwender**
- orientiert sich an den **GS-Katalogen des BSI** und an dessen Methodik
  - ⇒ angepasst/reduziert auf die Situation an der FU
- **konkrete Maßnahmen** für IT-Personal und für Anwender
- Erklärt den **IT-Sicherheitsprozess** an der FU
- Anleitung und Beispiel für **Schutzbedarfsanalyse**
- Anleitung und Beispiel für **Risiko- und Schadensanalyse**
- Seit Version 2.0/Sommer 2008 für den gesamten IT-Einsatz in allen Bereichen der Freien Universität Berlin verbindlich!

Empfehlungen & Tipps

- ☐ persönlich-fachlich „am Ball bleiben“
- ☐ Betrieb eines Rechners
- ☐ Werkzeuge (Auswahl/Beispiele)
- ☐ Routine? – Routine! (oder ...?)
- ☐ homogene IT
- ☐ Dokumentation
- ☐ Kommunikation
- ☐ Eskalation

Fachlich auf dem Laufenden bleiben

⇒ Informationsquellen (später im Vortrag)

⇒ aber: häufige Sicherheitslücken und Schwachstellen sind oft altbekannt und es existieren oftmals sogar bereits Patches/Updates dagegen – also...?!

Freie Universität Berlin

Betrieb eines Rechners

- Betriebssystem aktuell halten
  - ⇒ Version nutzen, für die es noch Sicherheits-Support vom Hersteller gibt
  - ⇒ regelmäßig, am besten automatisch, nach Updates suchen (lassen) (mind. 1x pro Woche)
- Sicherheits-Updates für Anwendungen regelmäßig einspielen
  - ⇒ regelmäßig, am besten automatisch, nach Updates suchen (lassen) (mind. 1x pro Woche)
- Antivirus-Software installieren und mind. 1x täglich die Virendefinitionen aktualisieren lassen
- regelmäßig Backups insbesondere der Daten anfertigen
  - ⇒ Das Betriebssystem und die übrige Software lassen sich meist (wenn auch ggf. mit einigem Aufwand) restaurieren oder neu beschaffen
- normales Arbeiten mit dem Rechner nur unter einem nicht-privilegierten Account

Freie Universität Berlin

Software-Werkzeuge

- Beispielhaft, ohne Anspruch auf Vollständigkeit:
  - ⇒ nmap
  - ⇒ tcpdump oder tshark (ggf. auch WLAN-Sniffer)
  - ⇒ OpenSSL
  - ⇒ SHA-1
  - ⇒ Bootfähiges System von CD (z.B. „Knoppicilin“)
  - ⇒ die **Textkonsole**! :-) (auch unter Windows und Mac OS X!)

Freie Universität Berlin

Routine! – Routine?

- Übung und Erfahrung helfen
  - ⇒ besonders in Stress-Situationen, in denen unter hohem Druck schnell gearbeitet werden muss (Incidents)
- Kehrseiten:
  - ⇒ fehlende Aufmerksamkeit, Desinteresse
  - ⇒ Selbstüberschätzung
  - ⇒ Monotonie

Freie Universität Berlin

Homogene IT-Landschaft

- Vorteile:
  - ⇒ bessere Wartbarkeit
  - ⇒ Einheitlichkeit
  - ⇒ besser automatisierbar
  - ⇒ SSO etc.
  - ⇒ Abhängigkeiten/Strukturen klarer

Freie Universität Berlin

Nachteile einer IT- „Monokultur"

- ggf. alle Systeme von einer Schwachstelle betroffen
- Einheitlichkeit macht es (auch) für einen *Angreifer* leichter
  - ⇒ aber: ist „security by obscurity" wirklich besser?
- größere Abhängigkeiten als bei heterogener IT-Landschaft?
  - ⇒"single point of failure"?!

Freie Universität Berlin

Dokumentation

- ungeliebt (vor allem bei Admins)
- meist kein *unmittelbarer* Nutzen für die Anwender („vertane Zeit") – aber!
- Arbeitszeit dafür einplanen

Freie Universität Berlin

Kommunikation

- Bedeutung oft unterschätzt
- Was will man beim Adressaten erreichen?
  - ⇒ Beherzigen von Hinweisen
  - ⇒ Verständnis für Notwendigkeit/Sinn und Akzeptanz von (unpopulären Sicherheits-)Maßnahmen
- in Krisenfällen besonders wichtig und zugleich schwierig
  - ⇒ intern ggü. Admin-Kollegen und/oder Chefs
  - ⇒ gegenüber Nutzern
  - ⇒ ggf. gegenüber Externen
- Vorbereiten
  - ⇒ Verteiler
  - ⇒ Textbausteine

Freie Universität Berlin

Eskalation

- Alarmierungsplan
  - ⇒ Wer kann ggf. helfen?
  - ⇒ Wer muss informiert/einbezogen werden?
- Kontakt-Infos
  - ⇒ Notfall-Telefonnummern
  - ⇒ auch in nicht-elektronischer Form!
- ggf. zumindest nachträglich

Freie Universität Berlin

Informationsquellen

- moderierte/redaktionell bearbeitete bevorzugen
  - ⇒ besser strukturiert
  - ⇒ thematisch oft schärfer fokussiert
  - ⇒ eher nach eigenen Bedürfnissen konfigurier- oder filterbar
  - ⇒ meist Gegenmaßnahmen und/oder eine Bewertung zu Schwachstellen oder Exploits mitgeliefert
  - ⇒ dürften für die meisten Anwendungsfälle ausreichend sein
  - ⇒ Nachteil: sind meist etwas langsamer
- auch nicht-elektronische Quellen/Foren/Kontakte wahrnehmen bzw. nutzen (Kontaktpflege, Vertrauensnetz)!
  - ⇒ Betriebstagungen, Stammtische, Konferenzen

Freie Universität Berlin

BSI

- „Bundesamt für Sicherheit in der Informationstechnik“ http://www.bsi.bund.de
  - ⇒ ehem. „Zentralstelle für das Chiffrierwesen“
  - ⇒ pflegt die Grundschutz-Kataloge
  - ⇒ gibt darüber hinaus Empfehlungen z.B. zu Krypto-Algorithmen und Schlüssellängen heraus
  - ⇒Newsletter „BSI für Bürger“

Freie Universität Berlin

DFN-CERT

- CERT = „Computer Emergency Response Team“
  - » inzwischen meist eher CSIRT = „Computer Security Incident Response Team“
- „Anlauf-, Koordinierungs- und Informationsstelle rund um IT-Sicherheitsthemen und -vorfälle“
- zentraler Ansprechpartner für Interne und Externe bei Missbrauch/Beschwerden (abuse) innerhalb oder aus dem Deutschen Forschungsnetz (DFN)
- www.dfn-cert.de
- Advisory-Dienst (deutschsprachig) win-sec-ssc (Mailingliste)
- Mirror mit Windows-Updates
- u.v.a.

Freie Universität Berlin

Heise Security (Heisec)

- www.heisec.de
- Newsticker (WWW/RSS)
- wöchentlicher E-Mail-Newsletter
- Grundlagen-Artikel
- SW-Sammlung
- Foren
- Dienste (u.a. Browsercheck)

Freie Universität Berlin

bugtraq-Mailingliste

- www.securityfocus.com
- unstrukturiert
- „Full disclosure" und gleichzeitig Diskussionsliste
  - ⇒ keine Unterstützung für automatische Filterung
  - ⇒ keine „Priorisierung" der Meldungen
  - ⇒ high volume! (> 3000/Jahr)

Freie Universität Berlin

Spezifische Sicherheits-Mailinglisten

- z.B. von Software-Herstellern
  - ⇒ MS, Apple, Linux-Varianten
  - ⇒ Anwendungssoftware
    - Hinweise auf Sicherheits-Updates der betreffenden Software
- Antivirus-Infos/-Warnungen
  - ⇒ z.B. NAI/McAfee („AvertLabs")

Freie Universität Berlin

SANS

- www.sans.org
  - ⇒ u.a. „SANS Top-20 Security Risks"
  - ⇒ vielfältige Online-Ressourcen

http://www.sans.org/top20/

Freie Universität Berlin

NSA

- National Security Agency www.nsa.gov
  - ⇒ Geheimdienst („No Such Agency" ;–)
  - ⇒ „America's cryptologic organization"
  - ⇒ weltgrößter Arbeitgeber für Mathematiker und Kryptologen
- Öffentliche Aktivitäten (u.a.)
  - ⇒ Entwickeln gehärtete OS-Varianten
    - SELinux
  - ⇒ Security Configuration Guides/Hardening Guides
  - ⇒ Mitwirkung bei Standardisierung, insbes. von Krypto-Algorithmen

Info-Quellen Recht

- DFN-Forschungsstelle Recht
  - ⇒ www.dfn.de/de/beratung/rechtimdfn/
- Gesetzesportal des Bundes
  - ⇒ www.gesetze-im-internet.de
- Bundesanzeiger www.bgbl.de
  - ⇒ kostenlose „nur-lese"-Versionen des Bundesgesetzblattes
- DIP – Dokumentations- und Informationssystem für Parlamentarische Vorgänge von Bundestag und Bundesrat
  - ⇒ http://dip21.bundestag.de
- Dokumentationssystem der Landesparlamente
  - ⇒ http://www.parlamentsspiegel.de

Aus der Praxis des Rechnerbetriebs...

- Heterogenität des FBs
- Sicherheitsmaßnahmen am FB MI
- häufigste Sicherheitsvorfälle
- aktuelle Sicherheitsvorfälle
- Doku + flexible Abfragemöglichkeit
- Checklisten
- Change-Management

Heterogenität

- User-Knowhow
- Anforderungen
  - ⇒ Standard-Büro-AP vs. „bleeding edge“ unstable/VISTA ...
- IT-Landschaft
  - ⇒ „historisch gewachsen“
  - ⇒ beschränktes Budget für Erneuerungen

Sicherheitsmaßnahmen

- ⇒ Separierung/Zonen
  - FB-Firewalls, DMZ, VPN-Firewall, separates Drucker-, FBV-/SichBK- und Technik-Netz
- ⇒ keine Dienste mit Klartext-Passworten
- ⇒ Prüfung auf schwache Passworte
- ⇒ Ablaufdatum für Benutzerkennungen
- ⇒ Dienstenutzung von selbstverw. Rechnern aus nur nach vorheriger Authentifizierung (VPN, Drucken; kein NFS)
- ⇒ Erkennung fremder Rechner (ARPwatch)
- ⇒ Least Privileges
  - Nutzeraccounts, separate Admin-Accounts, Win-Domänen-Richtlinien
- ⇒ Antivirus

Freie Universität Berlin

Häufigste Sicherheitsvorfälle

- Filesharing/Copyrightverletzungen
- „erbeutete" Passworte
- unvorsichtige Nutzer (Mail-Anhang, Software aus P2P-Netzen, Arbeiten als Admin)
- Rechner, die selten online sind (Laptops, Forschungssemester)
- schlecht gepflegte selbstverwaltete Systeme
  ⇒ Laptops, Rechner zuhause (VPN!), Experim.-Server
- schlecht gepflegte selbstverwaltete Software, insbesondere Content-Management-Systeme etc.
- unorganisierte/unkooperative Arbeitsgruppen
- Unaufmerksamkeit RB-Mitarbeiter

Freie Universität Berlin

Jüngere Sicherheitsvorfälle

- Debian-PRNG-Schwachstelle
- DNS Cache Poisoning-Schwachstelle
- kompromittierter AP-Rechner
- gelöschtes /import-Verzeichnis
- WiMi ohne Quota legt >1 Mio Dateien an
- Ausfall Klimatisierung

Freie Universität Berlin

Was fehlt/Verbesserungsbedarf?

- ☐ Doku
  - ⇒ flexible Abfrage-/Sortiermöglichkeiten
  - ⇒ daraus Benachrichtigungsmöglichkeit
  - ⇒ Bedarf z.T. a priori nicht absehbar
    - Debian PRNG-Bug (Schlüsselmaterial!)
- ☐ Checklisten
  - ⇒ eigene/angepasste
  - ⇒ standardisierte Vorgehensweise
- ☐ Change Management
  - ⇒ Mitarbeiter (RB / Sonstige)
  - ⇒ IT (Hardware, Software)

Freie Universität Berlin

Ansprechpartner an der FU

- ☐ am FB MI bei Sicherheits- und DS-Themen
  - ⇒ Ingmar <ingmar@mi...>, -75179
- ☐ IT-Verantwortliche/-r des Bereiches (FB MI: Carsten Schäuble)
- ☐ ZEDAT Netzgruppe/Abuse-Team/Hotline
  - ⇒ ag-netze@zedat.fu-berlin.de
  - ⇒ abuse@fu-berlin.de
  - ⇒ hilfe@zedat.fu-berlin.de
- ☐ Koordinator IT-Sicherheit: Dietmar Dräger
  - ⇒ dietmar.draeger@fu-berlin.de, Tel. -56572
- ☐ ggf. auch die Ermittlungsbehörden (Polizei/LKA/Staatsanwaltschaft)
- ☐ bei Datenschutzproblemen:
  - ⇒ FU-Datenschutzbeauftragte Ingrid Pahlen-Brand
    - datenschutz@fu-berlin.de, Tel. -53636
  - ⇒ Berliner Datenschutzbeauftragter
    - mailbox@datenschutz-berlin.de