



# Grundregeln: IT-Sicherheit im Forschungszentrum

D. Wesner, IT-Sicherheitsbeauftragter / IKM  
08. Oktober 2013



## Agenda

1. Motivation  
*Warum IT-Sicherheit?*
2. Grundlagen und Begriffe der IT-Sicherheit
3. Besonderheiten im FZJ
4. Vorfälle und Folgen  
*Was könnte schiefgehen?*
5. Der IT-Grundschutz des BSI
6. IT-Sicherheitskonzept des FZJ  
*„IT-Grundschutz angepasst an die Wissenschaft“*
7. Informationsquellen



## 1 Motivation: Warum IT-Sicherheit?

Maßnahmen zur IT-Sicherheit sind kontraproduktiv:  
Sie sind lästig, sie behindern mich bei der Arbeit\*,  
Daher kümmere ich mich nicht darum.

*\*(alles stimmt!)*



## 1 Analogie:

Maßnahmen zur IT-Sicherheit sind kontraproduktiv:  
Sie sind lästig, sie behindern mich bei der Arbeit,  
Daher kümmere ich mich nicht darum.

Sicherheitsgurte im Auto sind kontraproduktiv:  
Sie sind lästig beim Ein- und Aussteigen,  
sie behindern mich beim Lenken des Wagens,  
Daher kümmere ich mich nicht darum.







## 1 IT-Sicherheit ist für mich nicht relevant, weil...

### Argumente / Antworten:

- „Ich surfe selten im Internet...“
  - *Angriffe benötigen oft **keine aktive Mitwirkung** des Nutzers, sondern nur die Anwesenheit des Zielsystems im JuNet.*
- „Auf meinem Rechner ist kaum was drauf; selbst wenn er angegriffen würde, wäre der Schaden nicht groß...“
  - *Angreifer könnten ein übernommenes JuNet-System auch dafür benutzen, **Dritte anzugreifen***
- (oft von Wissenschaftlern) „Meine Forschung wird ohnehin veröffentlicht; ich habe keine Geheimnisse.“
  - ***Wirklich?** (neue Erkenntnisse vor der ersten Veröffentlichung, Information über einzigartigen Forschungsmethoden oder Geräten, strategische Überlegungen zu neuen Forschungsvorhaben, evtl. gespeicherte persönliche Daten, etc., etc.)*

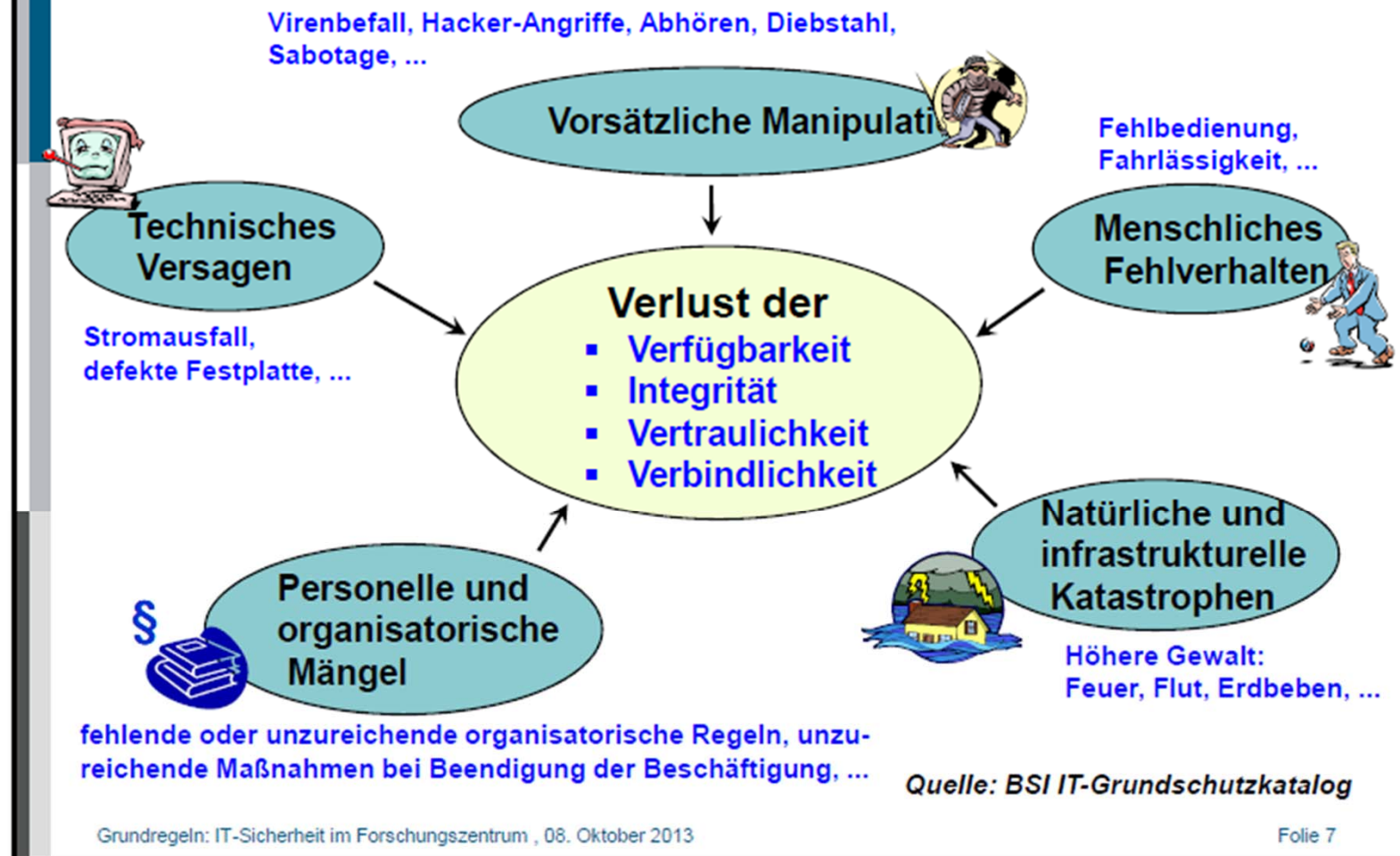
## 2 Grundlagen der IT-Sicherheit

- **Ziel:** IT-Ressourcen gegen Beschädigung ihrer Grundwerte zu schützen
  - Daten, Informationen
  - Hardware, Gebäude, Personal
  - Programme (Software), Prozesse
- Grundwerte von IT-Ressourcen sind
  - **Vertraulichkeit** → Einsicht ist nur für Befugte möglich
  - **Integrität** → ist durch Unbefugte nicht veränderbar
  - **Verfügbarkeit** → Befugten ist der Zugriff gewährleistet
  - **Verbindlichkeit** → Vorgänge sind nachvollziehbar, verifizierbar
- Bedrohungen / Gefahren:
  - Verursachen einen Verlust der Grundwerte
  - Werden durch **Maßnahmen** entgegengewirkt





## 2 Mögliche Bedrohungen einer IT-Ressource

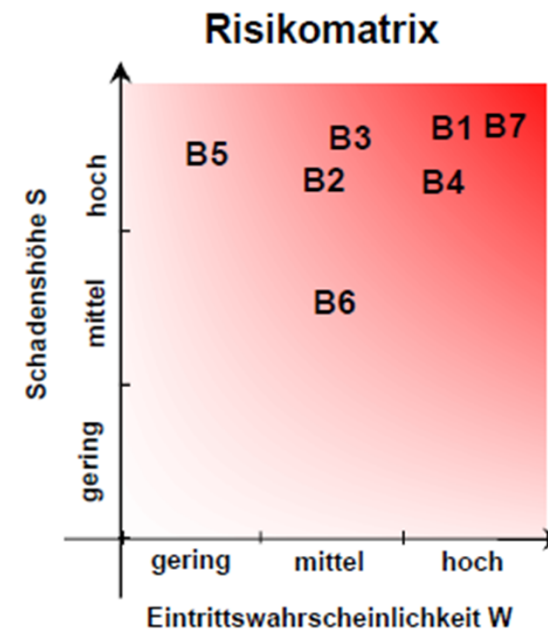




## 2 Risiko

- Risiko **R**
  - entsteht durch die Bedrohung **B**, die
  - einen Schaden der Höhe **S** mit der
  - Wahrscheinlichkeit **W** verursacht:

$$R = S \times W$$



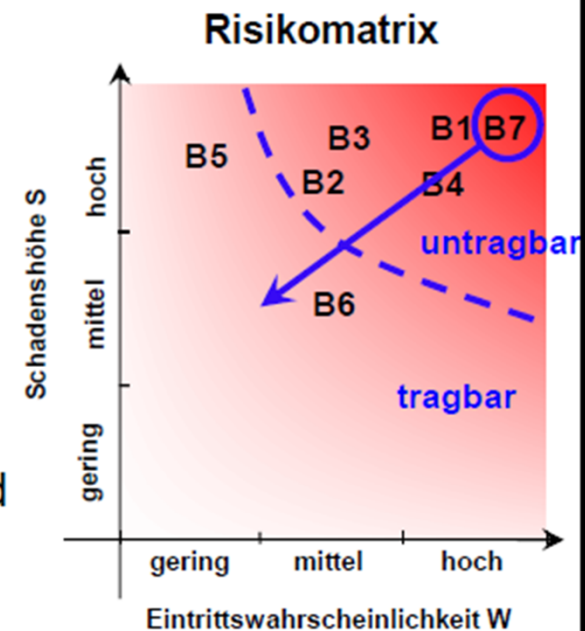


## 2 Risiko

- Risiko **R**
  - entsteht durch die Bedrohung **B**, die
  - einen Schaden der Höhe **S** mit der
  - Wahrscheinlichkeit **W** verursacht:

$$R = S \times W$$

- durch IT-Sicherheitsmaßnahmen wird das Risiko einer Bedrohung auf ein tragbares Niveau reduziert
  - „tragbar“ wird durch den Eigentümer der Ressource definiert...







### 3 Besonderheiten im FZJ

- **heterogene Nutzerschaft**
  - von „Verbrauchern“ von IT-Diensten bis hin zu erfahrenen, IT-versierten Anwendern
  - Aufenthaltsdauer: kurzzeitige Gäste, MA mit / ohne Zeitverträgen
- **hohes Bewusstsein und Verständnis** einzelner Nutzer für IT-Sicherheit - aber auch Gegenbeispiele
- oft **dezentral verwaltete, heterogene IT**  
(Ausnahmen: zentrale IT-Dienstleister JSC-KS, ITS, G-EN, O)
  - **dezentrale** Nutzer-Umgebungen (z.B. Stand-Alone Desktops)
    - *redundante, dezentrale Dienstleistungen (z.B. lokale Exchange-Server)*
  - hoher Anteil Nutzer mit **administrativen Rechten**
  - **Vielfalt / Unmenge** an Hardware, Software, Betriebssystemen

→ *nicht alles IT-Sicherheitsfordernd*



## 4 Vorfälle und Folgen: Was könnte schiefgehen?

- **Arbeitsaufwand** zur Wiederherstellung von Systemen
- **Ruf-Schädigung** (immaterielle Verluste)
  - Verlust von Fördermittel, Zurückhaltung bei Projektpartnern
- Verminderte **Arbeitsfähigkeit** der Nutzer
  - wichtige Dienste – z.B. E-Mail – nicht verfügbar
  - Datenverlust
- **Entgangene Gewinn** (finanzieller Verlust)
  - z.B. durch frühzeitiges Bekanntwerden patentierbarer Erfindungen
- **Juristische Folgen** (Bundesdatenschutzgesetz, KonTraG, ...)
  - Bußgeld, evtl. Freiheitsstrafe

→ *Folgen für den Einzelnen aber auch für die Allgemeinheit*



## 4 Vorfälle: Beispiele

- Verbreitung des Wurms „w32.sdbot“ 2006
  - bekannte, gepatchte Windows-Schwachstelle
  - 70 befallene Systeme in 25 OEen über 3-4 Tage
- Hackerangriff per SSH 2008
  - externer Angriff durch entwendete „Private Keys“
  - root-Rechten auf mehreren Servern erreicht, weiterführende Angriffe nach Innen und Außen
- „Phishing“-Mail 2012
  - an ca. 600 FZJ-Mailkonten gesendet
  - mehrere kompromittierte Konten mussten gesperrt werden (auch andere Konten wie VPN)







## 5 Der IT-Grundschutz des BSI: Grundidee

- Es gibt überall ähnliche
  - Geschäftsprozesse / Anwendungen (Einkauf, Personal, Finanz, ...)
  - IT-Systeme (Server, Clients, Serverraum, File-Shares, E-Mail...)
  - Bedrohungen und Risiken
- Daher ist eine pauschalisierte Betrachtung der Bedrohungen und geeigneten Gegenmaßnahmen oft ausreichend
  - jedenfalls für IT-Ressourcen mit Schutzbedarf „normal“
- Folge: klassische (aufwendige!) Risikoanalyse entfällt

→ Kurz:

*Standard-Sicherheitsmaßnahmen für standardisierte Systeme*



## 5 IT-Grundschutzkatalog

IT-Grundschutzkatalog (Ausgabe 2011)

- als PDF: 4068 Seiten
- Inhalt
  - 583 Gefährdungen „G“
  - 1327 Maßnahmen „M“
    - entsprechen Regeln oder „Best Practices“
  - 85 Bausteine „B“ (Modulen für typische Prozesse, Anwendungen, Komponenten, z.B. Mailserver, Webserver)
    - Zusammenfassung der Gefährdungslage
    - Empfehlung geeigneter Maßnahmen
    - Hinweise auf Vorgehensweise



Bundesamt  
für Sicherheit in der  
Informationstechnik

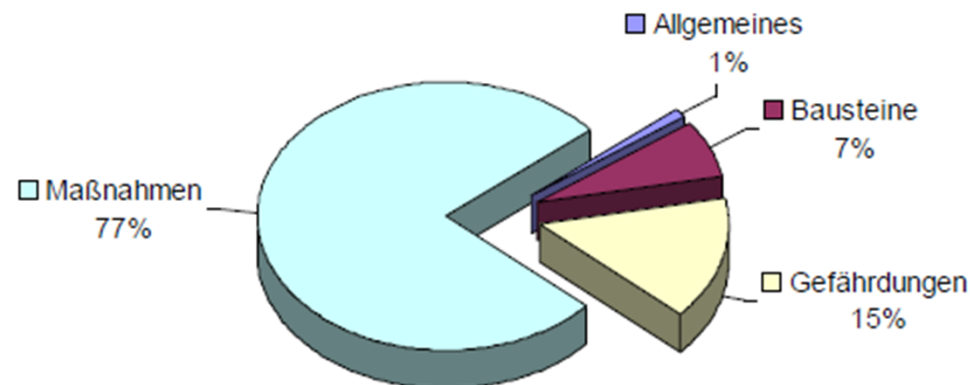




## 5 IT-Grundschutzkatalog

### *Verteilung der Kapitel im IT-Grundschutzkatalog*

- aus insgesamt 4068 Seiten:



- 2-3 A4-Seiten pro Maßnahme X 1327
- 1-2 A4-Seiten pro Gefährdung X 583
- 3-4 A4-Seiten pro Baustein X 85



## 5 Schutzbedarf im IT-Grundschutz

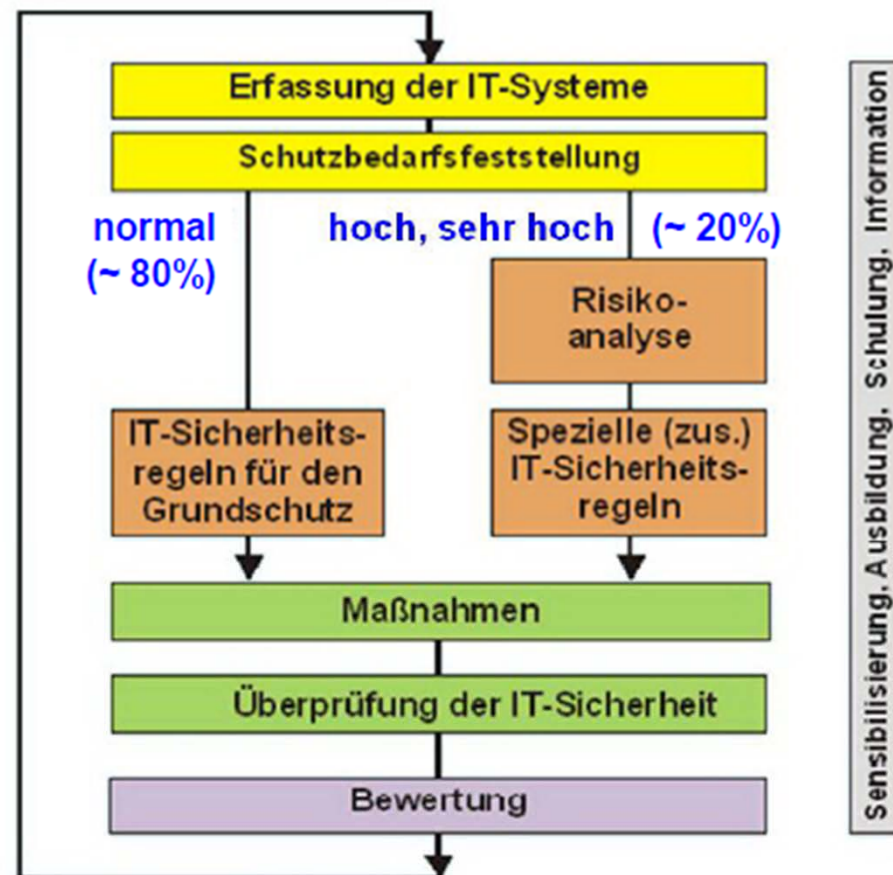
- Wichtige IT-Systeme werden zuerst **erfasst** und je nach **Schutzbedarf** in **IT-Schutzklassen** eingeteilt
  - abhängig von den Folgen eines Schadens

IT-Schutzklassen: exemplarische **Schadensfolgen**

- sehr hoch:** Arbeitsbeeinträchtigung nicht tolerabel (Ausfallzeit < 1 Std), **ruinöse Schäden** (Existenz bedrohend), Personenschäden, finanzielle Schäden > 10 Mio €
- hoch:** **erhebliche Beeinträchtigungen** der Arbeitsfähigkeit (Ausfallzeit 1 - 24 h), finanzielle Schäden > 2 Mio €, Personenschäden möglich
- normal:** **Beeinträchtigungen der Arbeitsfähigkeit tolerabel** (Ausfallzeit > 24 h), finanzielle Schäden tolerabel, Personenschäden ausgeschlossen



## 5 IT-Sicherheitsprozess im IT-Grundschutz



Grundregeln: IT-Sicherheit im Forschungszentrum, 08. Oktober 2013

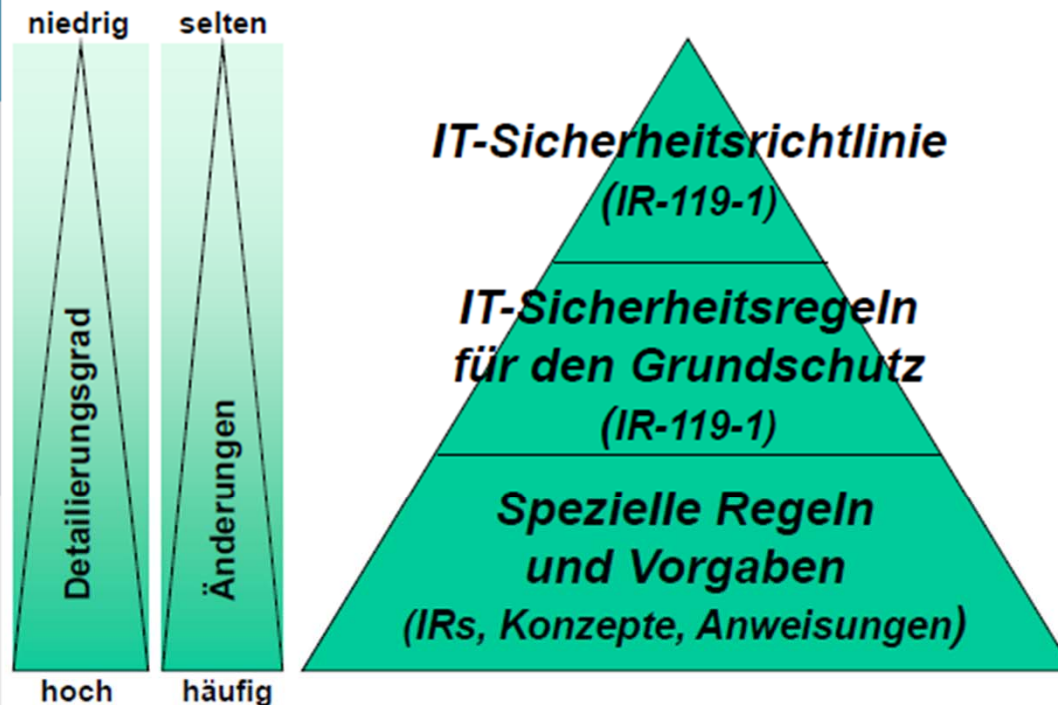
Folie 17





## 6 IT-Sicherheitskonzept des FZJ: „IT-Grundschutz angepasst an die Wissenschaft“

Dreistufiges Konzept:



„Politik“: Grundsätze,  
Begriffe und  
Organisation

„Konzept“: generelle  
Regeln (insges. 25)

bereichsspezifische  
oder spezialisierte  
Regeln



## 6 Generelle Prinzipien

- IT-Ressourcen sind wertvoll und zu schützen
- Offene Kommunikation hat Vorrang, sofern Sicherheitsbedürfnisse Dritter nicht beeinträchtigt werden
- Jeder ist verpflichtet, ein hohes Sicherheitsbewusstsein für die Risiken im eigenem Verantwortungsbereich zu haben
- IT-Ressourcen müssen entsprechend ihrem Schutzbedürfnis durch geeignete Sicherheitsmaßnahmen geschützt sein; Auswahl der Maßnahmen analog zum IT-Grundschutz:
  - normaler Schutzbedarf: IT-Sicherheitsregeln für den Grundschutz generell ausreichend (pauschalisierte Betrachtung)
  - hoher oder sehr hoher Schutzbedarf: detaillierten Bedrohungs- und Risikoanalyse erforderlich



## 6 IT-Grundschutzregeln im FZJ

### *Kategorien von Regeln:*

zur Infrastruktur	<b>I1 - I2</b>
zur Organisation	<b>O1 - O3</b>
zum Personal	<b>P1 - P3</b>
für Daten	<b>D1 - D4</b>
zur Hardware und Software	<b>H1 - H7</b>
zur Kommunikation	<b>K1 - K3</b>
zur Notfallvorsorge	<b>N1 - N3</b>

- Kategorien basieren auf Kategorien im **IT-Grundschutzkatalog** des BSI (bis auf „Daten“)
- Verglichen mit Anzahl der IT-Grundschutz-Maßnahmen (1327), **viel weniger FZJ-Regeln** (25) ...





## 6 Beispiel: Regeln H1-H3 zur Hardware und Software

**H1:** Jedes IT-System und jede Benutzerumgebung muss durch ein Passwort oder ein anderes starkes Authentifizierungsverfahren geschützt werden. Ein Passwort muss geheim und darf nicht erratbar sein.

**keine Namen, Daten, Wörter, Default-Passwörter, ...**

**H2:** Dienste ohne Passwortschutz oder ohne ein anderes starkes Authentifizierungsverfahren dürfen nur mit zusätzlichen Schutzmaßnahmen aktiviert werden. Nicht benötigte Dienste (z.B. Web-Server, FTP-Server) sind zu deaktivieren.

**keine offene Netzwerk-Freigaben; Pflicht zur System-„Härtung“**

**H3:** Die Betriebs- und Anwendungs-Software der IT-Systeme ist in einem sicherheitstechnisch guten Zustand zu halten. Vom IT-Sicherheitsbeauftragten als notwendig deklarierte Sicherheitsrelevante Software-Updates müssen installiert werden. Ist dieses nicht möglich, müssen die entsprechenden Sicherheitslücken in Absprache mit dem IT-Sicherheitsbeauftragten durch andere Maßnahmen beseitigt werden.

**(möglichst automatischer) Online-Update bei Windows, Linux**



## 6 Abgeleitete spezielle Regel aus Regel H3

- Bei „Skype“ sind besondere Maßnahmen nötig, um IT-Systeme „in einem sicherheitstechnisch guten Zustand zu halten“
- Hintergrund: Gefahr durch die verschlüsselten **Peer-to-Peer Netzwerkverbindungen**, die die Software zu Fremdsystemen aufbaut
  - insbesondere beim Übergang ins „SuperNode“-Modus
- Daher: **technische Einstellungen** der Skype-Client-Software
  - Verhindern „SuperNode“-Modus
  - Beschränken den Netzwerkverkehr
  - Begrenzen den Zugriff auf andere Programme des Rechners
- Maßnahmen für den Einsatz von Skype im JuNet als **Interne Regelung IR 122-2** veröffentlicht



## 7 Informationsquellen

- Bereich „IT-Sicherheit“ auf dem IT-Portal:
  - [http://intranet.fz-juelich.de/IT-Portal/DE/Home/home\\_node.html](http://intranet.fz-juelich.de/IT-Portal/DE/Home/home_node.html)
  - aktuelle IT-Sicherheitsthemen, Grundlagen (Richtlinien, Regeln, Schutzbedarf)
- JSC IT-Sicherheits-Portal:
  - [http://www.fz-juelich.de/ias/jsc/DE/Leistungen/Dienstleistungen/IT-Sicherheit/itsicherheit\\_node.html](http://www.fz-juelich.de/ias/jsc/DE/Leistungen/Dienstleistungen/IT-Sicherheit/itsicherheit_node.html)
  - Dokumentation („TKI“), aktuelle Warnungen
- Internet (**kleine** Auswahl):
  - Heise Security: <http://www.heise.de/security/>
  - Microsoft Security Response Center: <http://blogs.technet.com/b/msrc/>
  - BSI: [https://www.bsi.bund.de/DE/Home/home\\_node.html/](https://www.bsi.bund.de/DE/Home/home_node.html/)
  - Krebs on Security: <http://krebsonsecurity.com/>
  - Internet Storm Center: <https://isc.sans.edu/diary/>



Fragen?

