



Integriertes Management von Sicherheitsvorfällen

Stefan Metzger, Dr. Wolfgang Hommel, Dr. Helmut Reiser

18. DFN Workshop „Sicherheit in vernetzten Systemen“

Hamburg, 15./16. Februar 2011

Leibniz-Rechenzentrum

Was verstehen **wir** unter einem Sicherheitsvorfall?



❑ ISO27001-Definition: *Sicherheitsvorfall*

Ereignis, das sich **negativ** auf die Sicherheit, insbesondere auf die **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** von Informationen und Systemen, auswirkt.

❑ LRZ Security-Monitoring:

- Extern → Intern (Angriffe von Extern, DoS, SSH-Scans)
- Intern → Extern (Kompromittierte interne Systeme)

Angriffsziel „Hochschule“?



University Databases In the Bull's Eye

Recent wave of university hacks nationwide exposes vestiges of former practice of using social security number as identifiers

In March, 2008, Harvard University said a computer hacker gained entry to its server and that about 10,000 of the previous year's graduate students and applicants may have had their personal information compromised, with 6,600 having their Social Security numbers exposed. The school said it would provide the applicants with free identity theft recovery services and help them with credit monitoring and fraud alerts.

At the University of Missouri, a computer hacker accessed the Social Security numbers of more than 22,000 current or former students in May 2007, the second such attack that year, officials said. The hacker obtained the information through a Web page used to make queries about the status of trouble reports to the university's computer help desk, which is based in Columbia. The information had been compiled for a report, but the data had not been removed from the computer system.

Angriffsziel:
Personenbezogene Daten

Angriffsziel „Hochschule“?



University Databases In the Bull's Eye

Recent wave of university hacks nationwide exposes vestiges of former practice of using social security number as identifiers

In March, 2008, Harvard University said a computer hacker gained entry to its server and that about 10,000 of the previous year's graduate students and applicants may have had their personal information compromised, with 6,600 having their Social Security numbers exposed. The school said it would provide the applicants with free identity theft recovery services and help them with credit monitoring and fraud alerts.

At the University of Missouri, a computer hacker accessed the Social Security numbers of more than 22,000 current or former students in May 2007, the second such attack that year, officials said. The hacker obtained the information through a Web page on the university's computer help desk, which had been hacked, but the data had not been removed from the database.

Main Target of Cyberattacks Was a Professor

August 8, 2009, 10:00 am

A 34-year-old economics professor from the republic of Georgia appears to be the main target of a series of orchestrated cyberattacks Thursday and Friday on the Web services Twitter and Facebook, [The New York Times reports](#). The professor, who reportedly teaches at Sukhumi State University and blogs under the name Cyxymu, would identify himself only as "Giorgi."

Angriffsziel:
Forschungsdaten

Das Leibniz-Rechenzentrum (LRZ)



- ❑ RZ für Münchner Hochschulen, Betreiber MWN
- ❑ „Landesrechenzentrum“ und nationales Höchstleistungsrechenzentrum



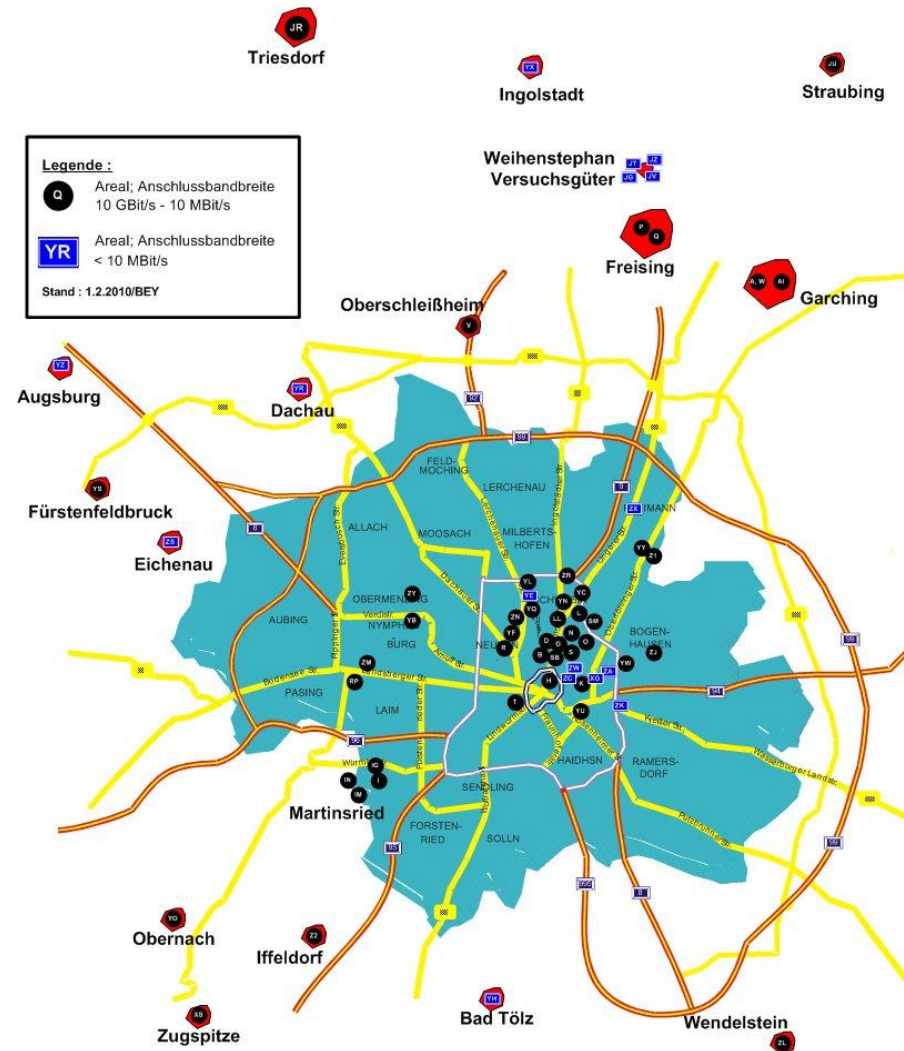
Foto: Ernst A. Graf

Münchner Wissenschaftsnetz (MWN)

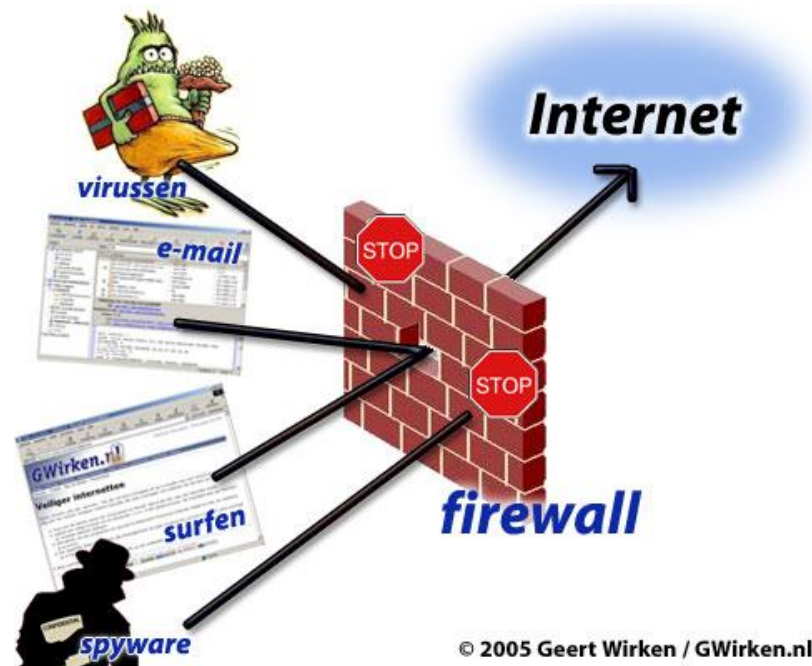
Eckdaten



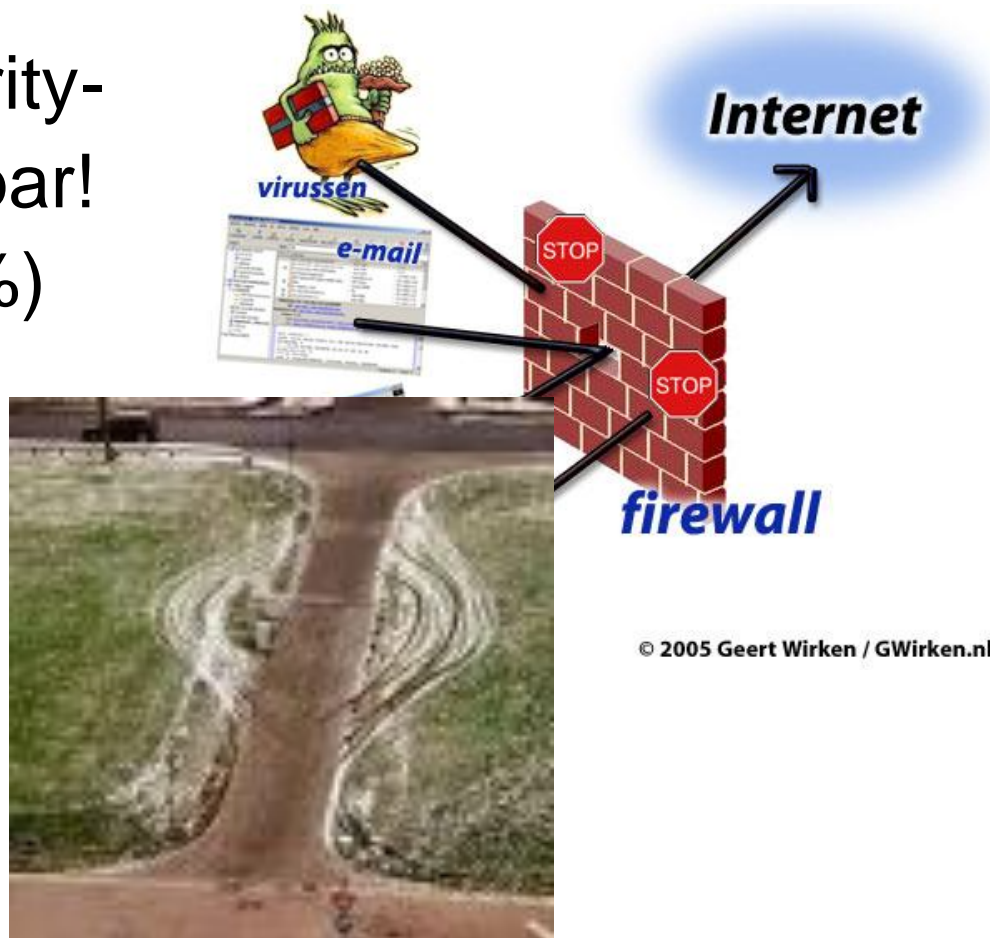
- ❑ 120.000 Nutzer
- ❑ ca. 80.000 Endgeräte
- ❑ Bayernweite Ausdehnung
- ❑ Dezentrale Administration und Verantwortlichkeit



- ☐ Installation von Security-Patches nicht forcierbar! (Infektionsrate: 1 - 5%)
- ☐ Firewalls
- ☐ Intrusion Detection / Prevention Systeme



- ☐ Installation von Security-Patches nicht forcierbar! (Infektionsrate: 1 - 5%)
- ☐ Firewalls
- ☐ Intrusion Detection / Prevention Systeme



- ❑ Installation von Security-Patches nicht forcierbar!



Präventive Schutzmaßnahmen greifen im MWN zu kurz und können nicht erzwungen werden!

- ❑ Intrusion Detection / Prevention Systeme



© 2005 Geert Wirken / GWirken.nl

Integrierte, reaktive Maßnahmen nötig!



Zielsetzungen:

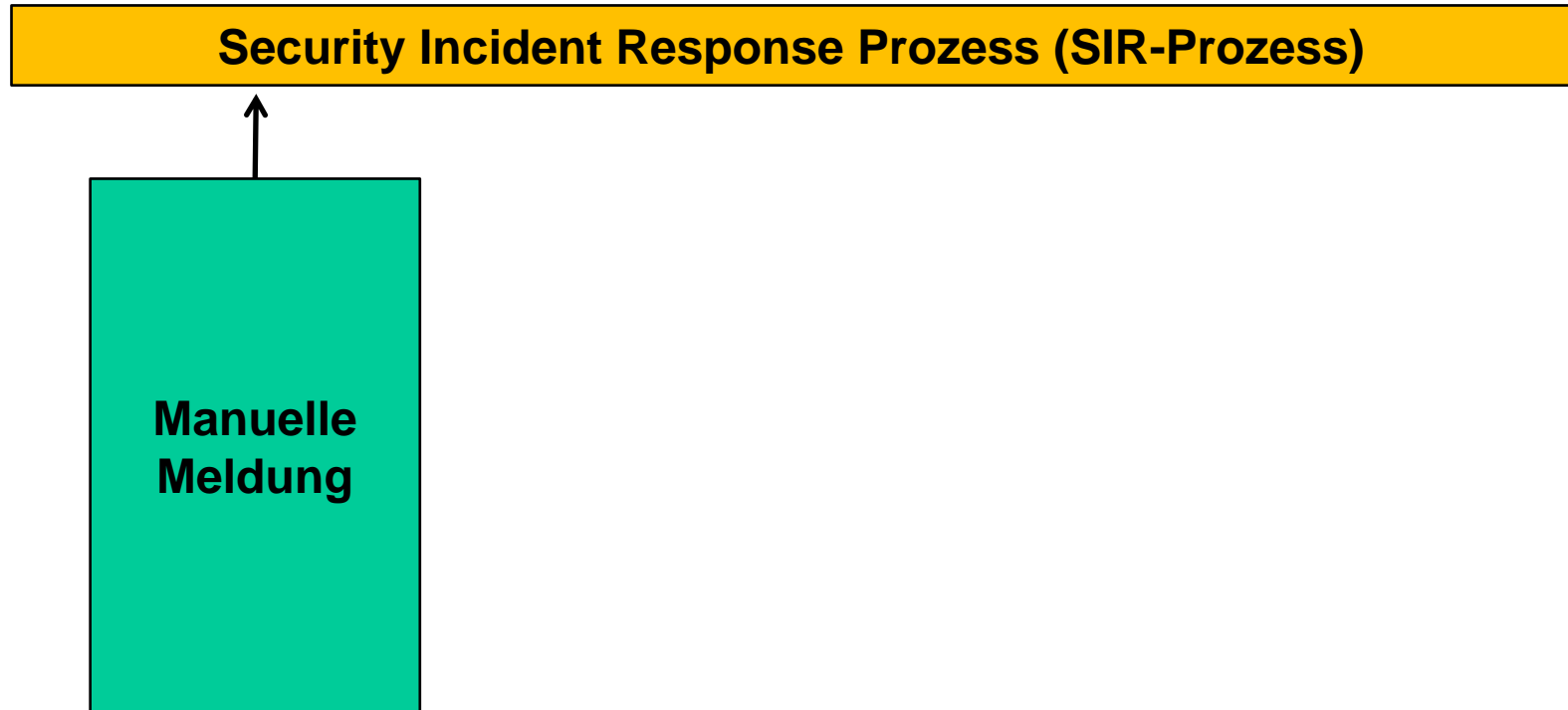
- Strukturierte Bearbeitung!
- Klare Regelung der Verantwortlichkeiten!
- Automatisierte Reaktions-Möglichkeiten!

Integrierte, reaktive Maßnahmen nötig!

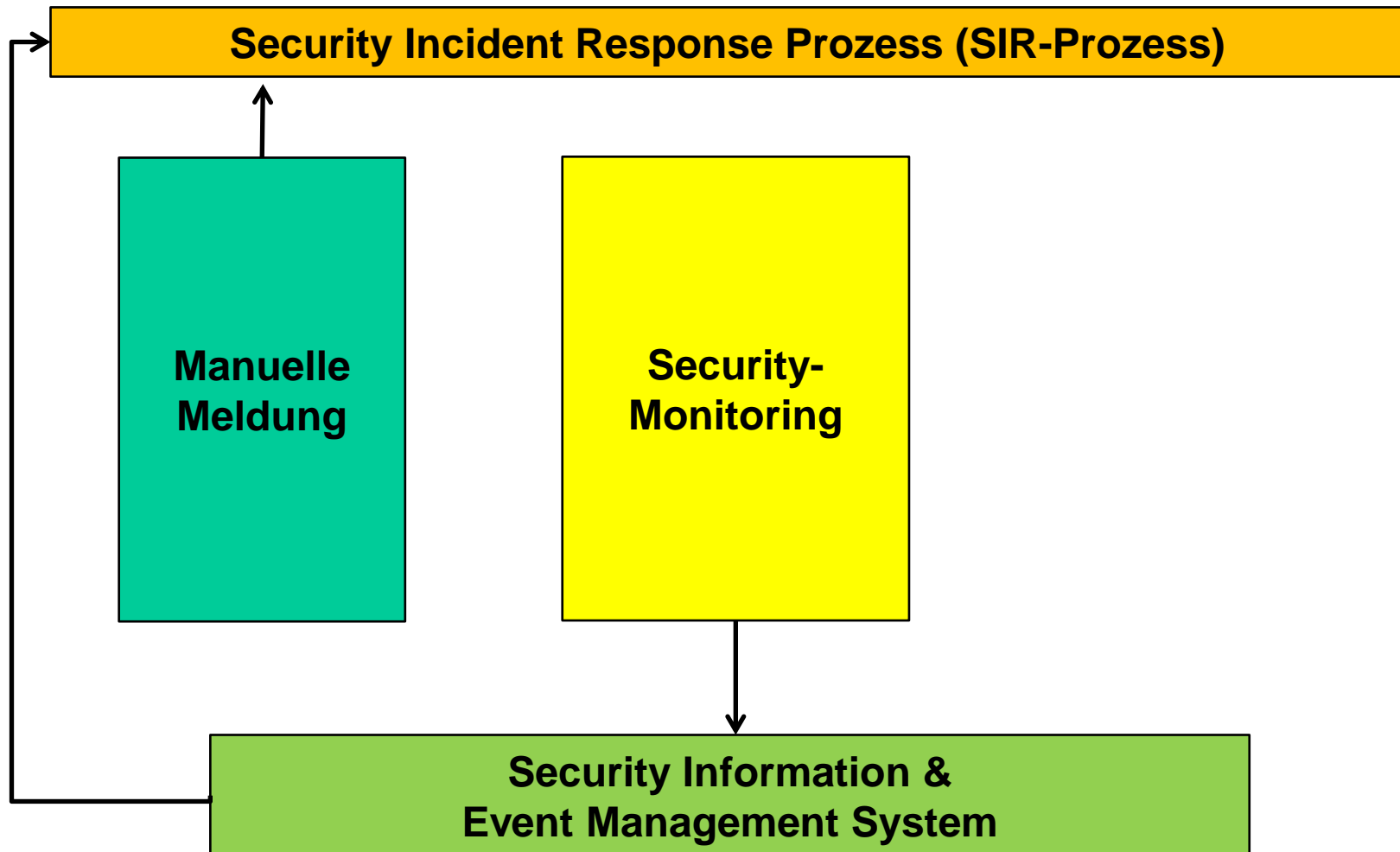


Security Incident Response Prozess (SIR-Prozess)

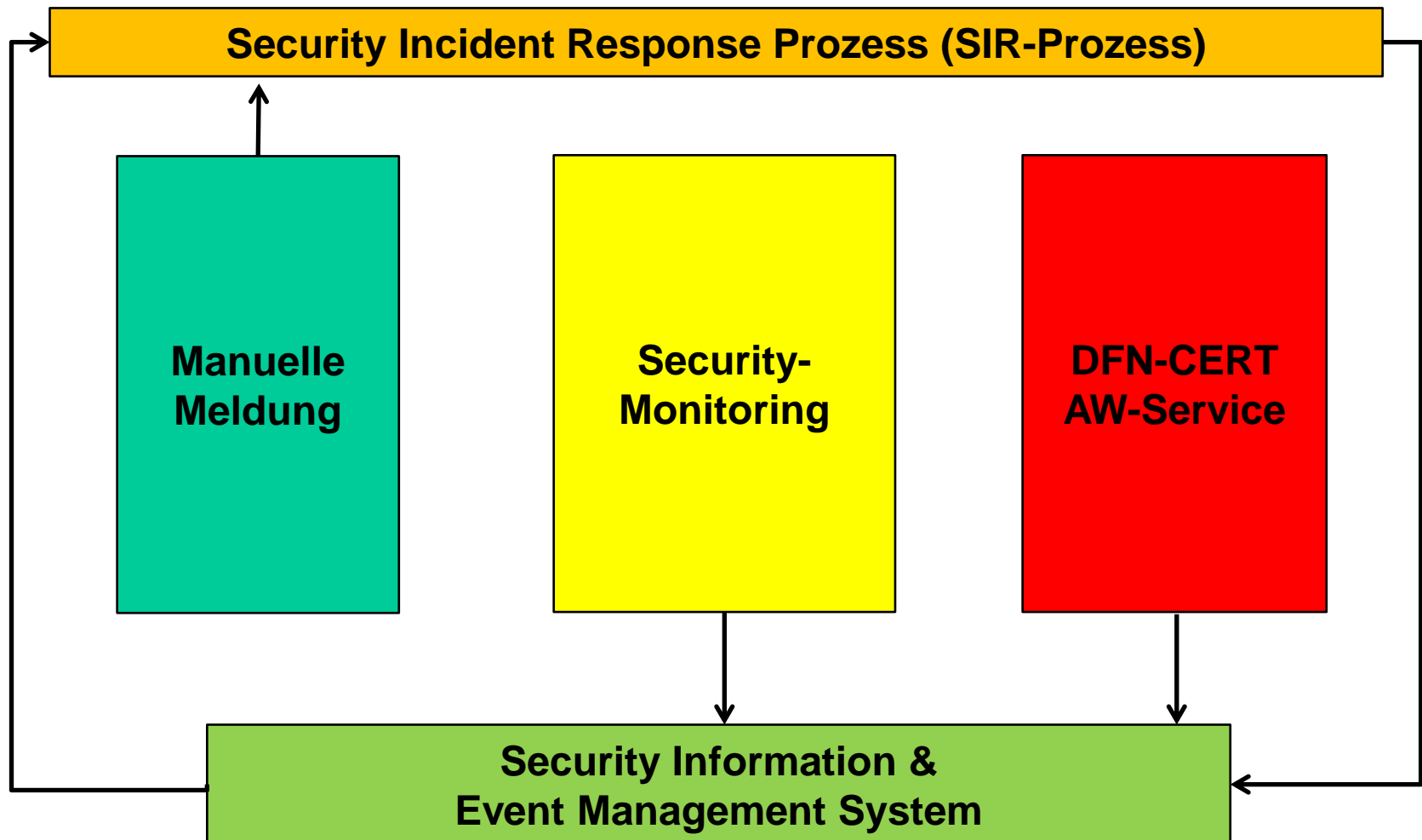
Integrierte, reaktive Maßnahmen nötig!



Integrierte, reaktive Maßnahmen nötig!



Integrierte, reaktive Maßnahmen nötig!



Tool-gestütztes Security Monitoring



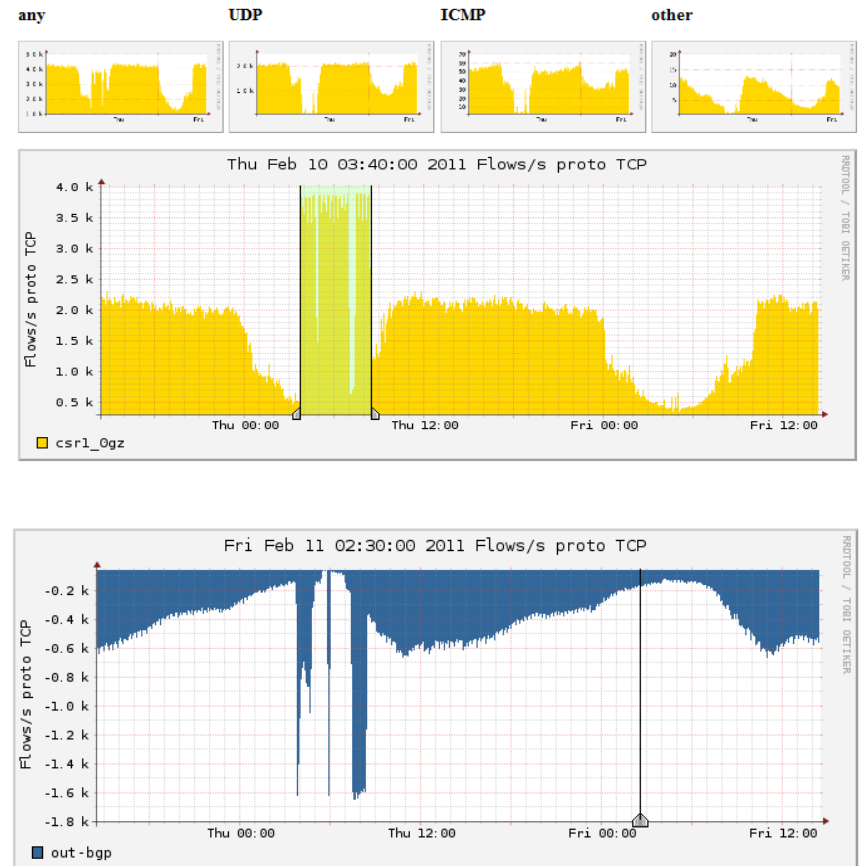
☐ SNORT IDS



☐ NfSEN (Netflow-Analyse)

☐ Accounting
(SPAM-Sender, DoS)

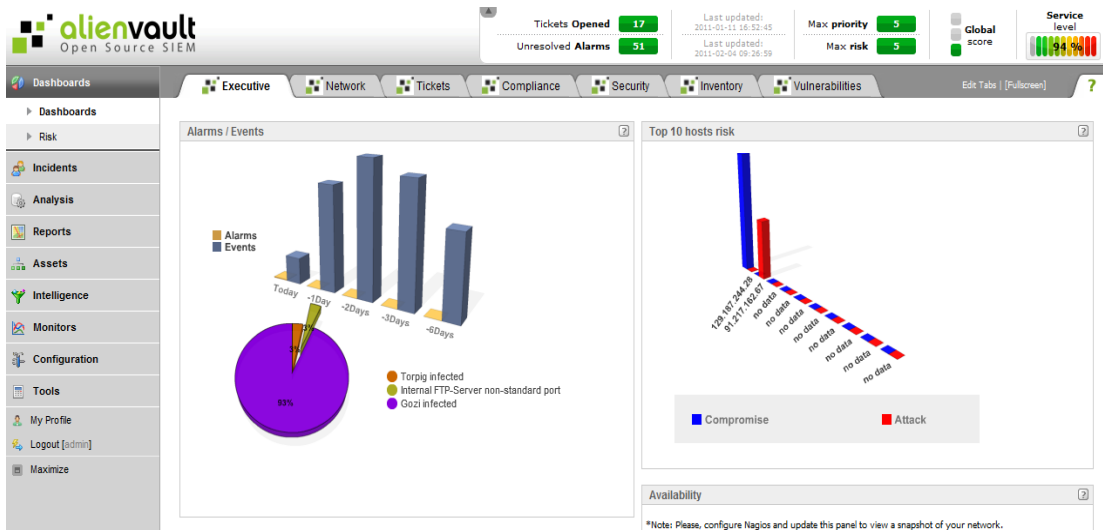
☐ NAT-o-MAT / Secomat



Security Information & Event Management (SIEM)



Open Source SIM (OSSIM)



☐ Dashboards

☐ Reporting-Funktionen

☐ Event-Korrelation

☐ Automatische Reaktion

Security Information & Event Management (SIEM)




Integrierte Sortier- und Filter-Funktionen



Open Source SIM (OSSIM)

- Unique Events
- Source- / Destination (IP oder Port)
- Zeitfenster

Search | Clear

search term  **IP** Signature Payload

Sensor Data Sources Risk




► More Filters



Time frame selection:

Today | Last 24 Hours | Last Week | Last two Weeks | Last Month | All

► Displaying unique source addresses 1-14 of 14 matching your selection. 39,341 total events in database.

Current Search Criteria [...Clear All Criteria...]				
META	PAYLOAD	IP	LAYER 4	
Signature " snort: "ET TROJAN Downadup/Conficker A or B Worm reporting"" ...Clear...	any	any	none	
time >= [06 / 22 / 2010] [any time] ...Clear...				

Summary Statistics			
Events	Sensors	Unique Events 	Unique Plugins
Unique addresses:  	Source Port:	Destination Port:	Unique IP links [FQDN]
Source Destination	TCP UDP	TCP UDP	Unique Country Events

Src IP address	Sensor #	▲ Total # ▼	Unique Events	Dest. Addr.
 138.246.2.108 	1	624	1	14

DFN-CERT Services

Automatische Warnmeldungen



- ☐ Sensoren beim DFN-CERT
- ☐ DFN-Einrichtungen werden täglich über auffällige IP-Adressen informiert

Meldungen:

IP	Meldungstyp	Zuletzt gesehen

129.xxx.xxx.xxx	Bot	2011-02-12 14:06:03 GMT+0100

DFN-CERT Services

Automatische Warnmeldungen



- ☐ Sensoren beim DFN-CERT
- ☐ DFN-Einrichtungen werden täglich über auffällige IP-Adressen informiert

Details zu den Meldungen pro IP:

System: 129.xxx.xxx.xxx

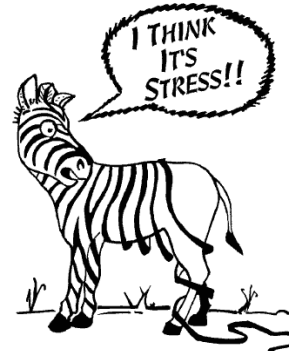
Meldungstyp: Bot

Zeitstempel: 2011-02-12 14:06:03 GMT+0100 (Sommerzeit) >

Protokoll	Quellport	Zielpport	Malwaretyp	Zeitstempel(GMT+0000)
-----------	-----------	-----------	------------	-----------------------

unbekannt		6667	unbekannt	2011-02-12 13:06:03
unbekannt		6667	unbekannt	2011-02-12 13:06:03

Nach Bekanntwerden eines Vorfalls ...



Security Incident Response Prozess

Incident Aufnahme

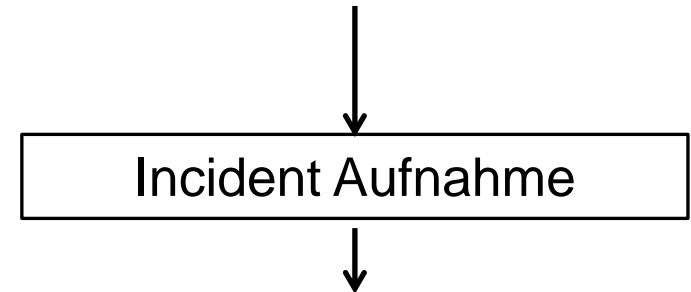


☐ **Was** ist genau passiert?

☐ **Welches** System ist betroffen?

☐ **Wer** ist für System zuständig?

☐ **Wann** ist es passiert?



Security Incident Response Prozess

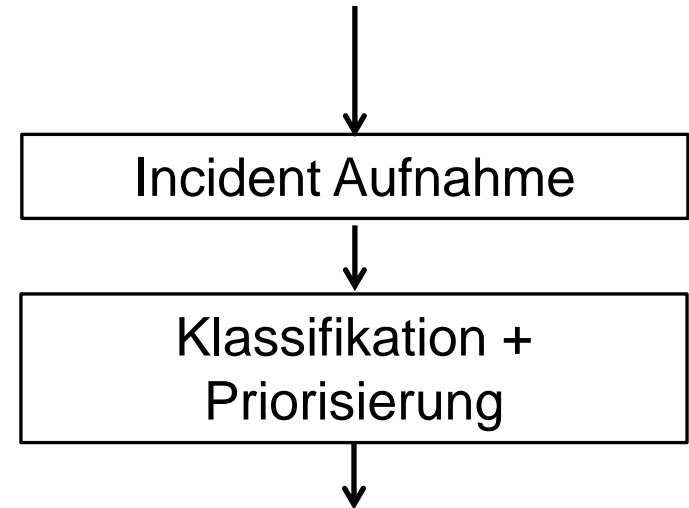
Klassifikation + Priorisierung



❑ Welche Art von Angriff?

❑ **Priorisierung** des Vorfalls

- Standort des Angreifers?
- Standort des Opfer-Systems?
- Wieviele Systeme sind betroffen?
- Welche Dienste sind betroffen?



Security Incident Response Prozess

Klassifikation + Priorisierung



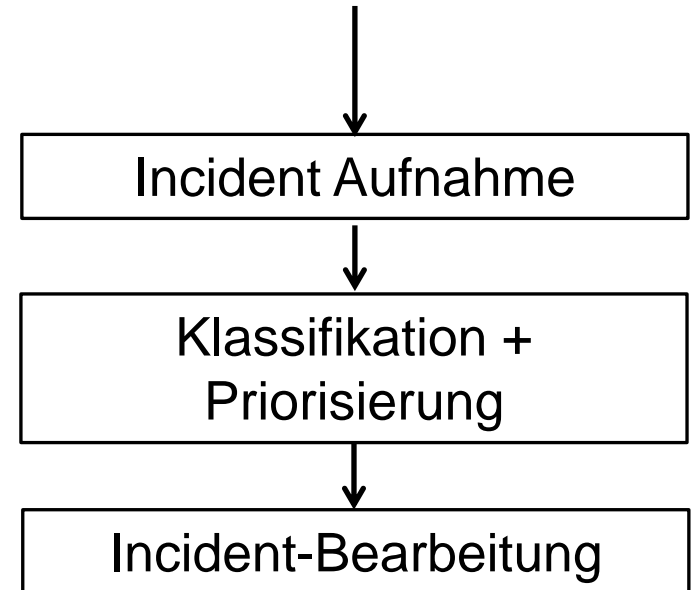
Auswirkung/ Kriterium	Niedrig	Mittel	Hoch
Zielsystem	Extern (1)	MWN, Grid (2)	LRZ-intern (3)
Dienste, Daten	nicht betroffen (1)	MWN, Grid (2)	Wichtige Dienste (3)
# betroffener Systeme	1 (1)	2-3 (2)	> 3 (3)
Quellsystem	Extern (1)	MWN, Grid (2)	LRZ-intern (3)

Security Incident Response Prozess

Incident-Bearbeitung



- ❑ Standard-Security-Incident?
→ definierte Vorgehensweise
- ❑ Erstmaßnahmen
- ❑ Analyse & Diagnose
betroffener Systeme

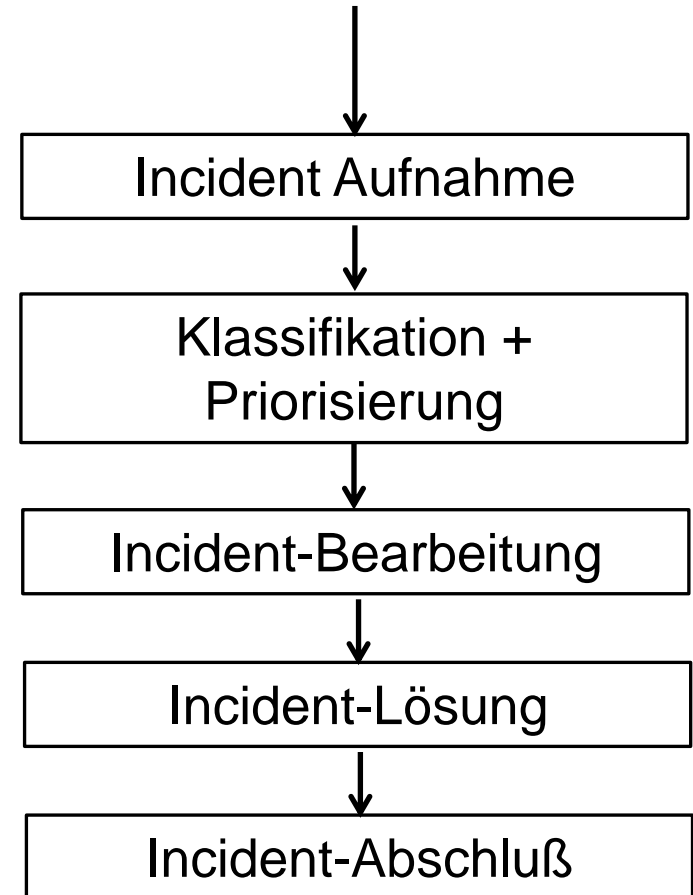


Security Incident Response Prozess

Lösung + Abschluß des Incidents



- ☐ Schnellstmögliche Lösung des Incidents
- ☐ Wiederherstellung Regelbetrieb
- ☐ Weitere Auffälligkeiten?
- ☐ Abschluß (Post Incident Review)



Security Incident Response am LRZ

Beispiel



- ☐ SNORT IDS detektiert Event (Bot C&C Server Traffic)
- ☐ Weiterleitung an SIEM

snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 13:05:14	129. [redacted] [German flag] [Bot icon]	194. [redacted] :6667 [Hungarian flag]
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 12:04:52	129. [redacted] [German flag] [Bot icon]	195. [redacted] :6667 [Finnish flag]
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 11:04:40	129. [redacted] [German flag] [Bot icon]	194. [redacted] :6667 [Hungarian flag]
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 10:02:50	129. [redacted] [German flag] [Bot icon]	194. [redacted] :6667 [Hungarian flag]
snort: "ET DROP Known Bot C&C Server Traffic TCP (group 15) "	2011-02-12 09:02:08	129. [redacted] [German flag] [Bot icon]	194. [redacted] :6667 [Hungarian flag]

- ☐ Korrelation (mind. 5 Events / 8 Stunden) → Alarm!

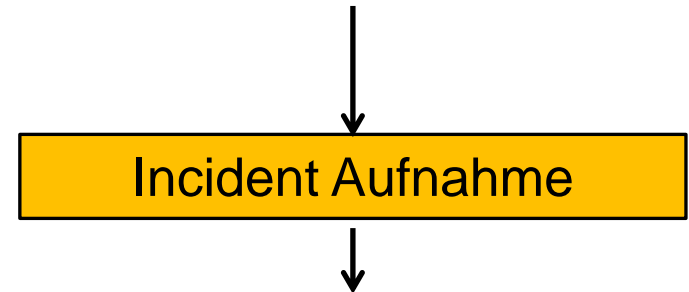
Security Incident Response am LRZ

Beispiel



Nach dem Alarm →

- Security-Incident Ticket erzeugen
- System-Administratoren + LRZ-CSIRT informieren



Security Incident Response am LRZ

Beispiel



Event: **snort: "ET DROP KNOWN BOT C&C Server Traffic TCP"**

IP-Adresse: 129.xxx.xxx.xxx

FQDN: <HOSTNAME>

Standort: <STANDORT (Gebäude, Adresse)>

Switchport:
<SWITCH-PORT DETECTION>

Source-Port: xxxxx

Destination-IP: 194.xxx.xxx.xxx

Destination-Port: 6667

Timestamp: Sat Feb 12 13:05:14 2011

Security Incident Response am LRZ

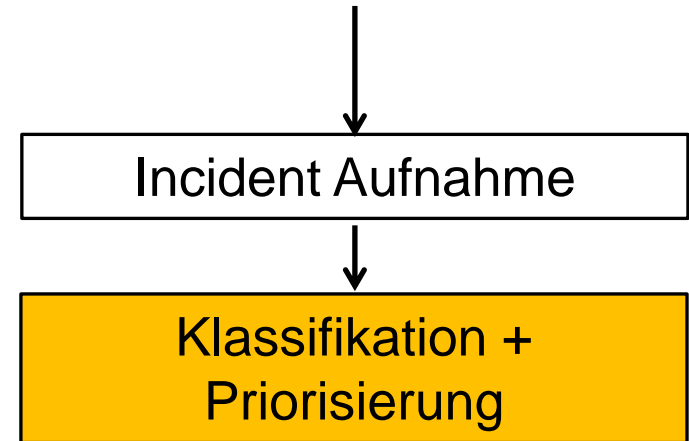
Beispiel



❑ **Klassifikation:**

- Botnetz C&C-Server
- Intern → Extern!

❑ **Priorisierung:**



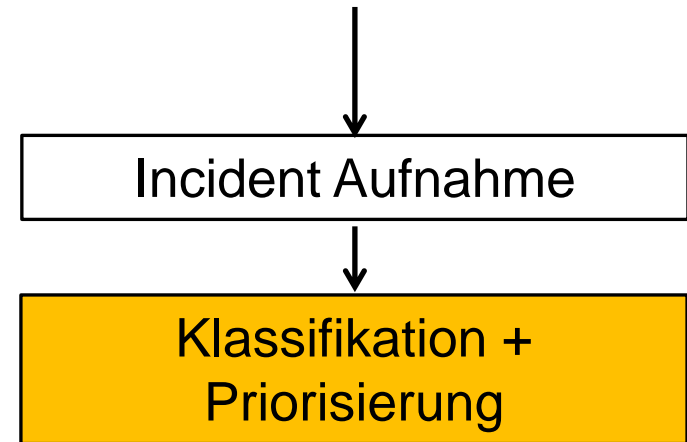
Security Incident Response am LRZ

Beispiel



□ Klassifikation:

- Botnetz C&C-Server
- Intern → Extern



□ Priorisierung:

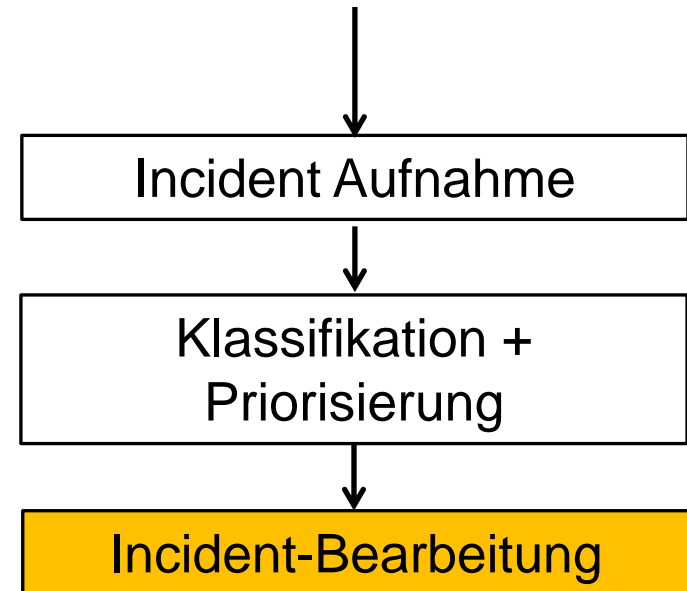
Zielsystem	Extern (1)	Grid, MWN	Intern
Dienste	Nein (1)	Grid, MWN	Ja
# Systeme	1 (1)	2,3	mind. 3
Quellsystem	Extern	Grid, MWN	Intern (3)

Security Incident Response am LRZ

Beispiel



DFN AW-Service Meldung:
Bestätigung des internen
Monitorings



Meldungen:

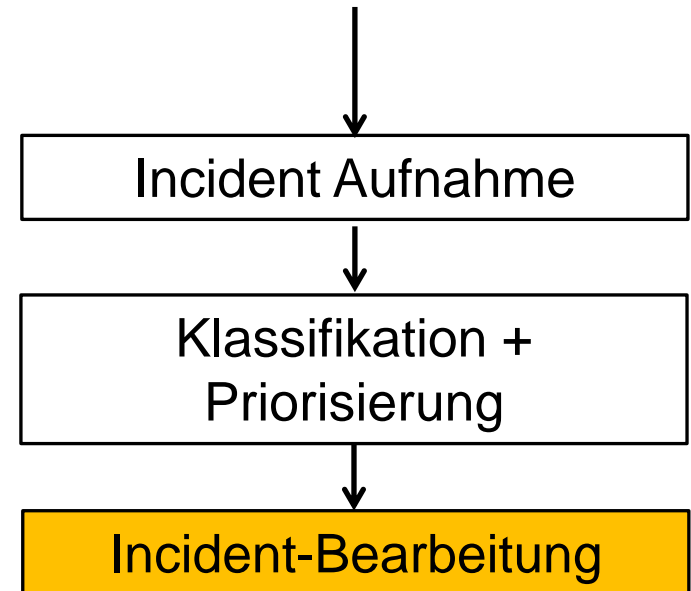
IP	Meldungstyp	Zuletzt gesehen
129.xxx.xxx.xxx	Bot	2011-02-12 14:06:03 GMT+0100

Security Incident Response am LRZ

Beispiel



- ❑ **Erstmaßnahme**
Trennen der Netzverbindung
- ❑ **Analyse & Diagnose:**
 - Auswertung SIEM-Events
 - Analyse der Log-Files



Security Incident Response am LRZ

Beispiel



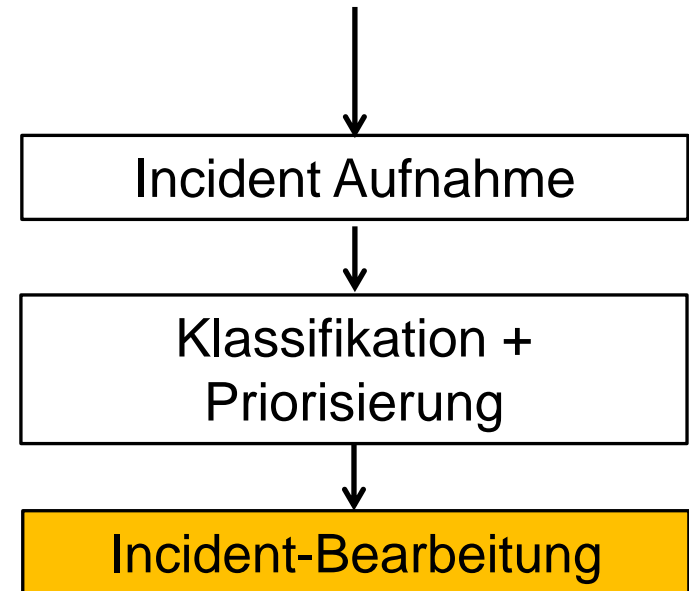
❑ **Auswertung SIEM-Events**

(10.02.2011)

„External SSH-Attacker“ auf
Destination 129.xxx.xxx.xxx

❑ **Analyse der Log-Files**

- SSH-Login von externer IP-Adresse erfolgreich
- Kennung „test“ mit Passwort „test123!“
- Root-Exploit
- Installation einer Bot-Software



Security Incident Response am LRZ

Beispiel

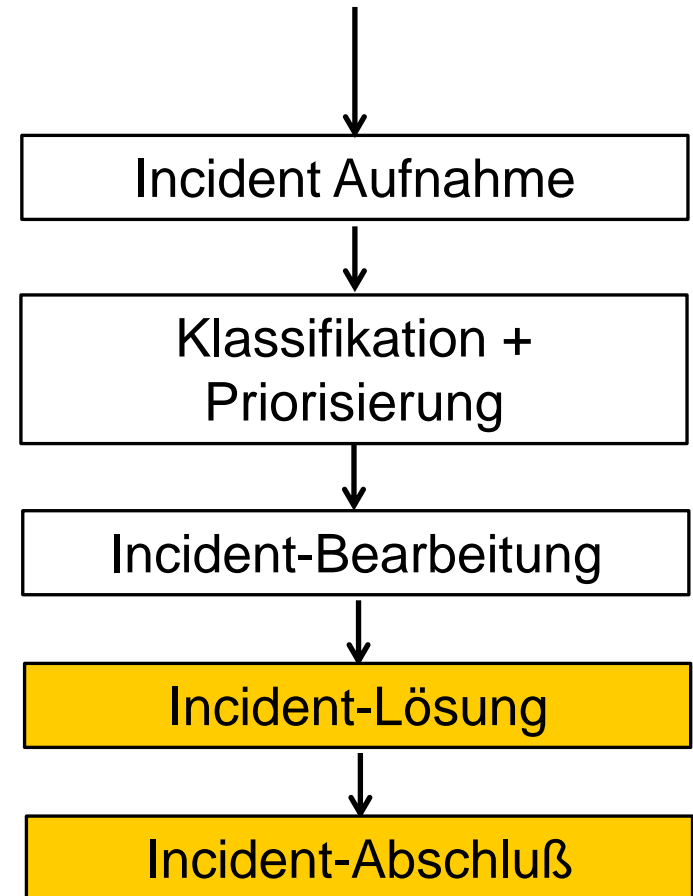


- ❑ **Lösung:**
Neuinstallation des Systems!

- ❑ **Abschluß (PIR):**

Bei dieser Art von Vorfall zukünftig:

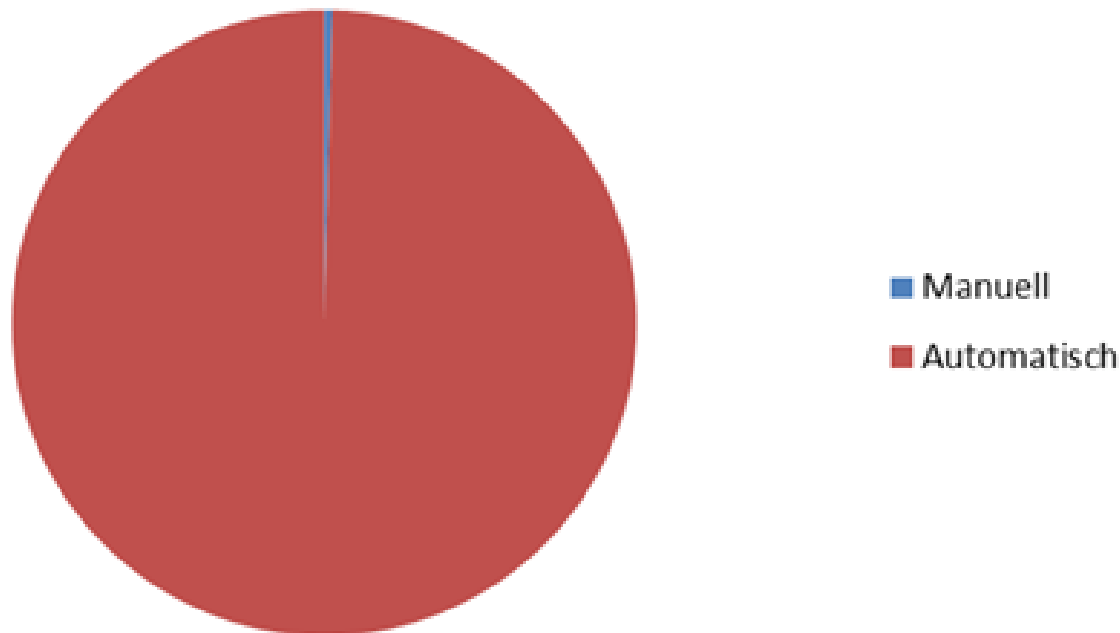
„**Automatisches Blocking**“



2010:

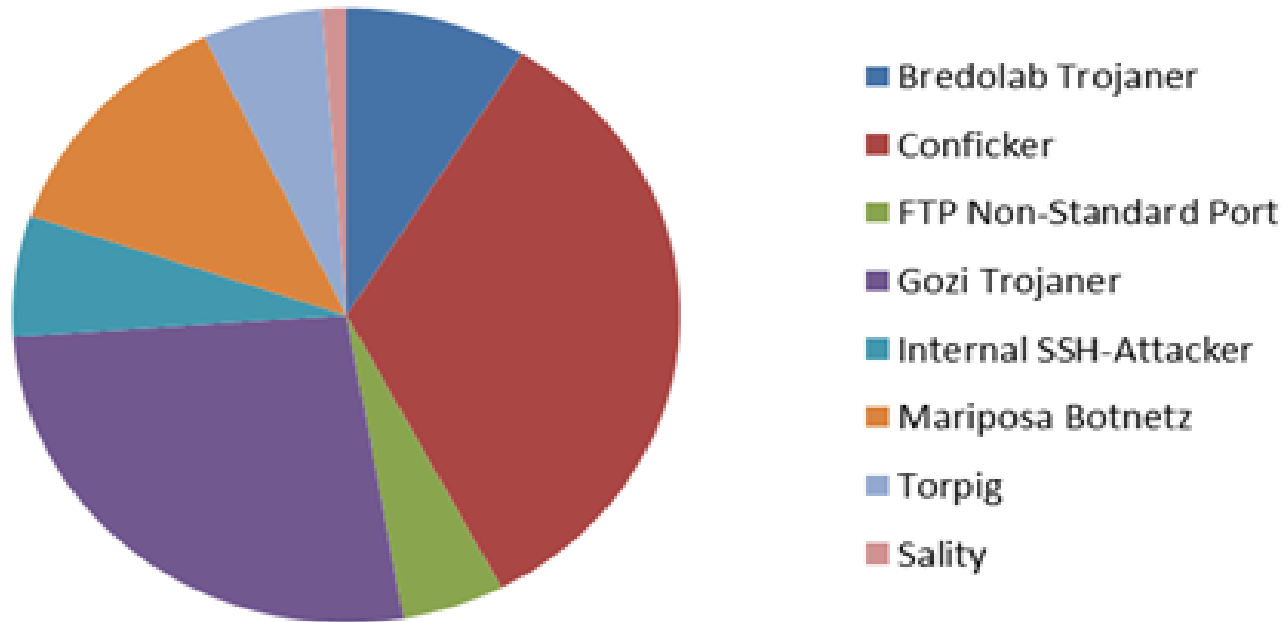
Insgesamt **935** Vorfälle: 99,6 % automatisch!

Verteilung Manuell/Automatisch

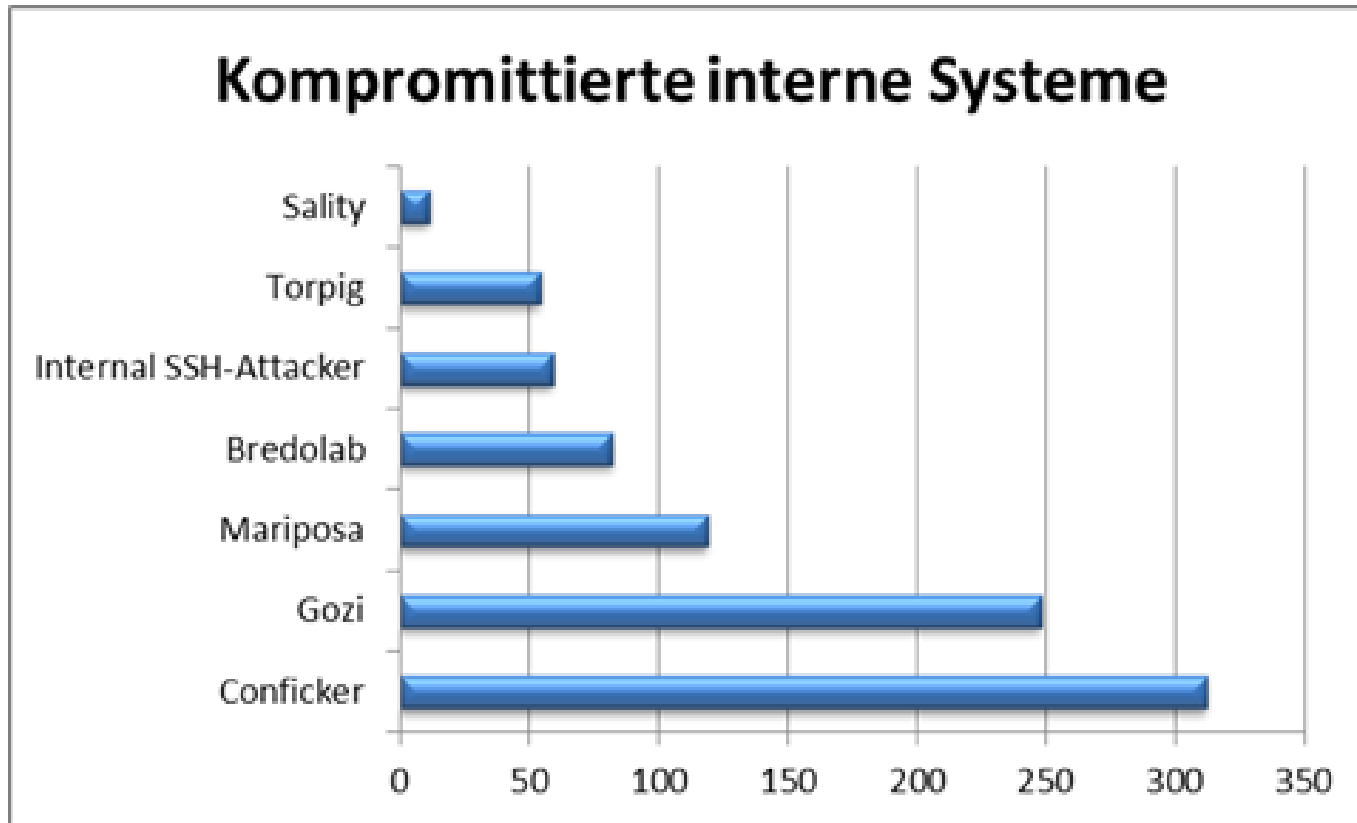


2010: Kompromittierte Interne Systeme

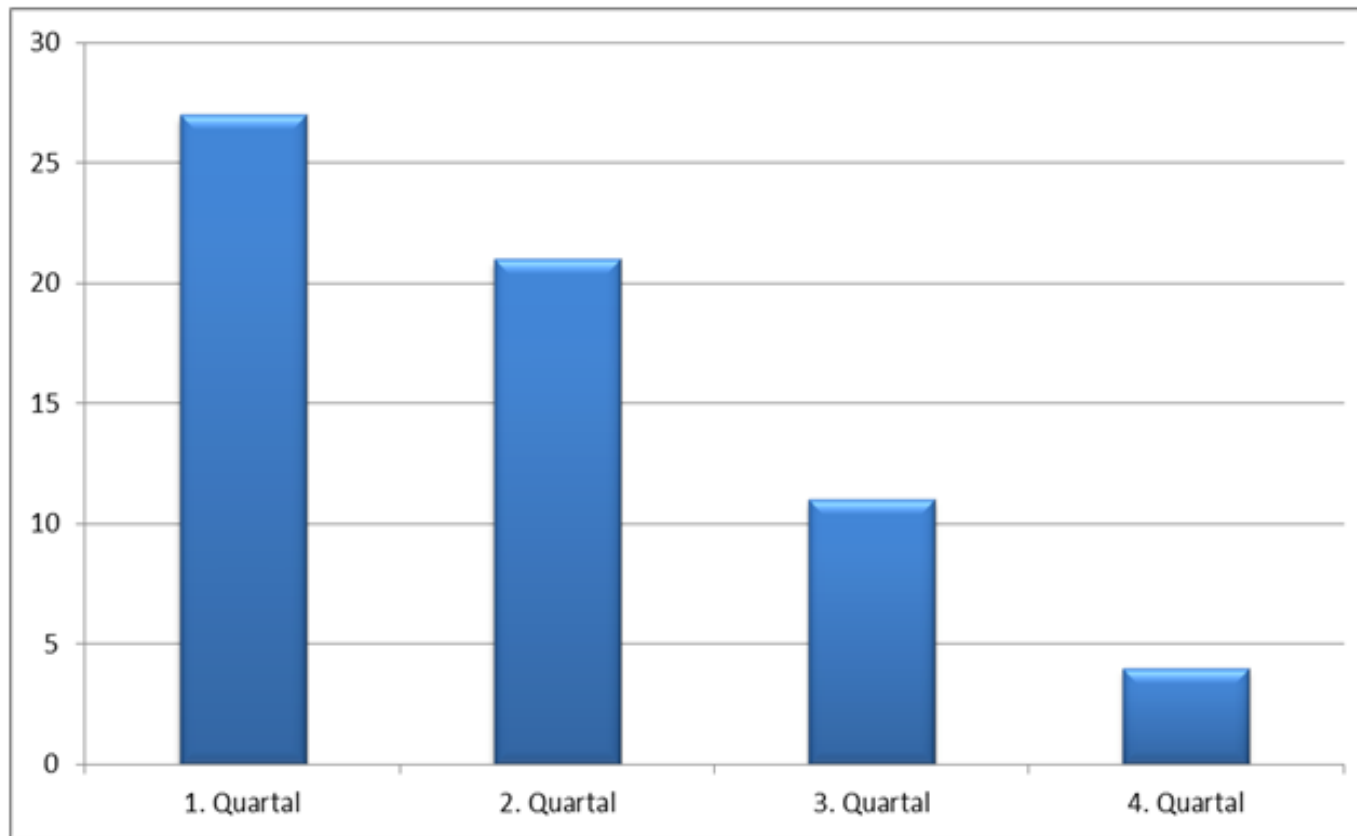
Welche Art von Vorfall?



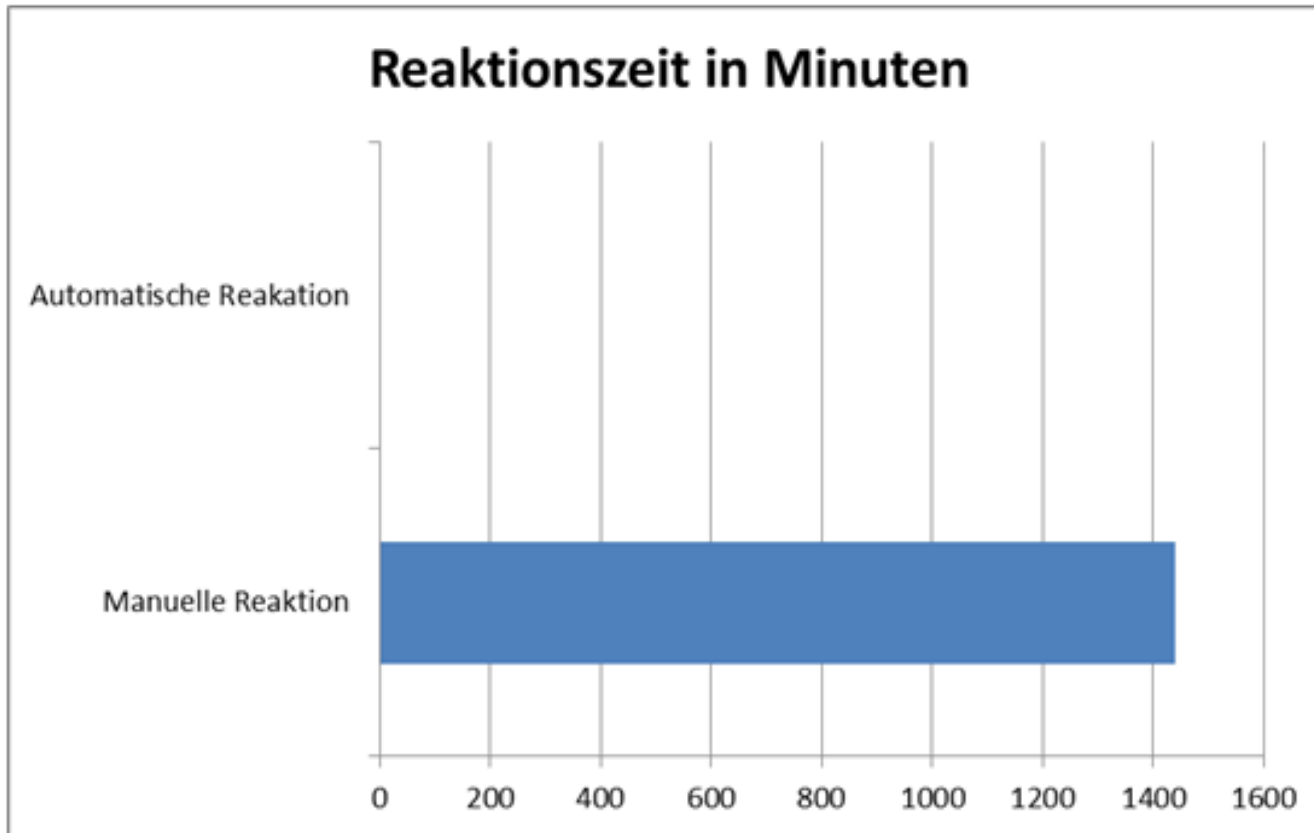
2010: Kompromittierte Interne Systeme



Anzahl IP-Adressen in DFN-CERT AW-Meldungen



Reaktionszeit



Fragen?

