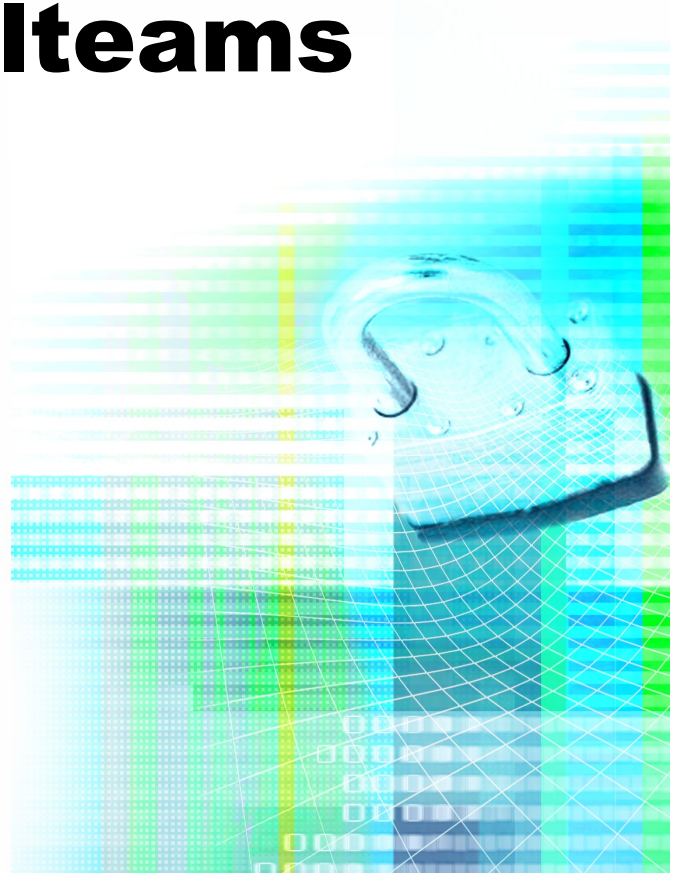
DFN CERT

IT-Sicherheitsteams / Computer-Notfallteams in der Praxis



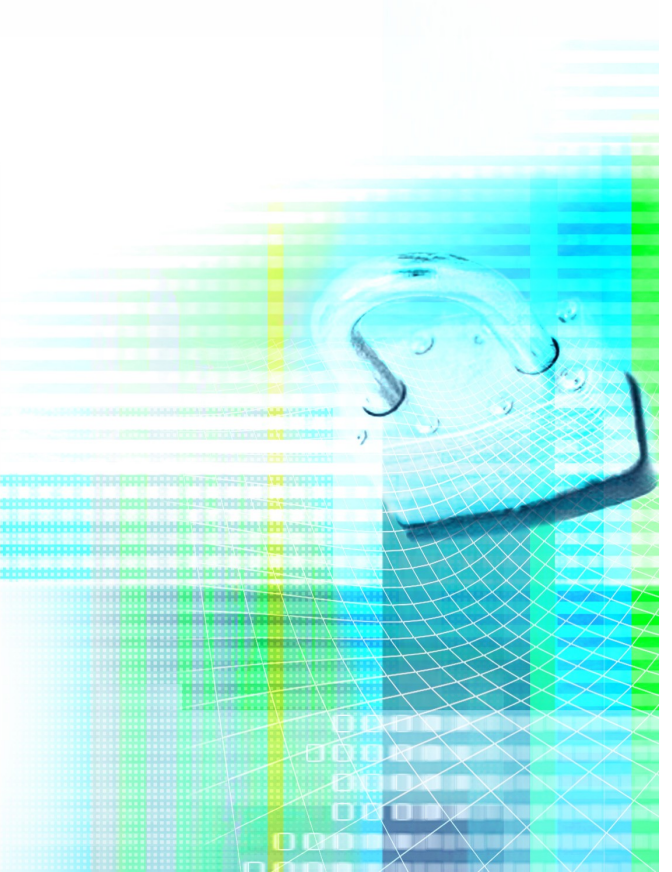
Dr. Klaus-Peter Kossakowski
klaus-peter@kossakowski.de

Agenda

- Das DFN-CERT
- Die klassischen Säulen der CERT-Arbeit
  - Proaktive Komponenten
  - Reaktive Komponente
  - Noch frühere Warnung
- CERTs im nationalen und internationalen Verbund
- Was machen Unternehmen?

DFN CERT

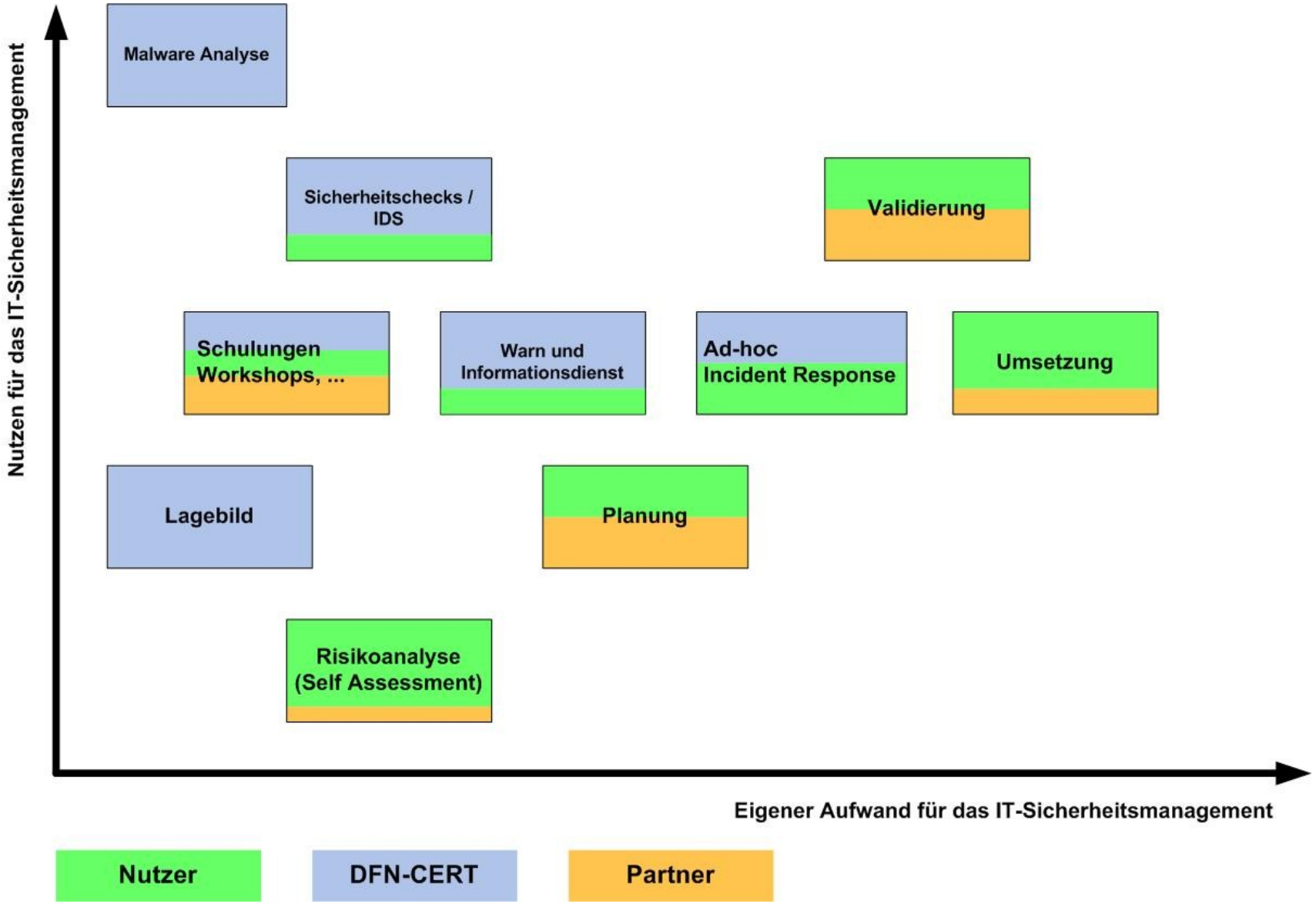
DFN-CERT: Entstehung und Entwicklung

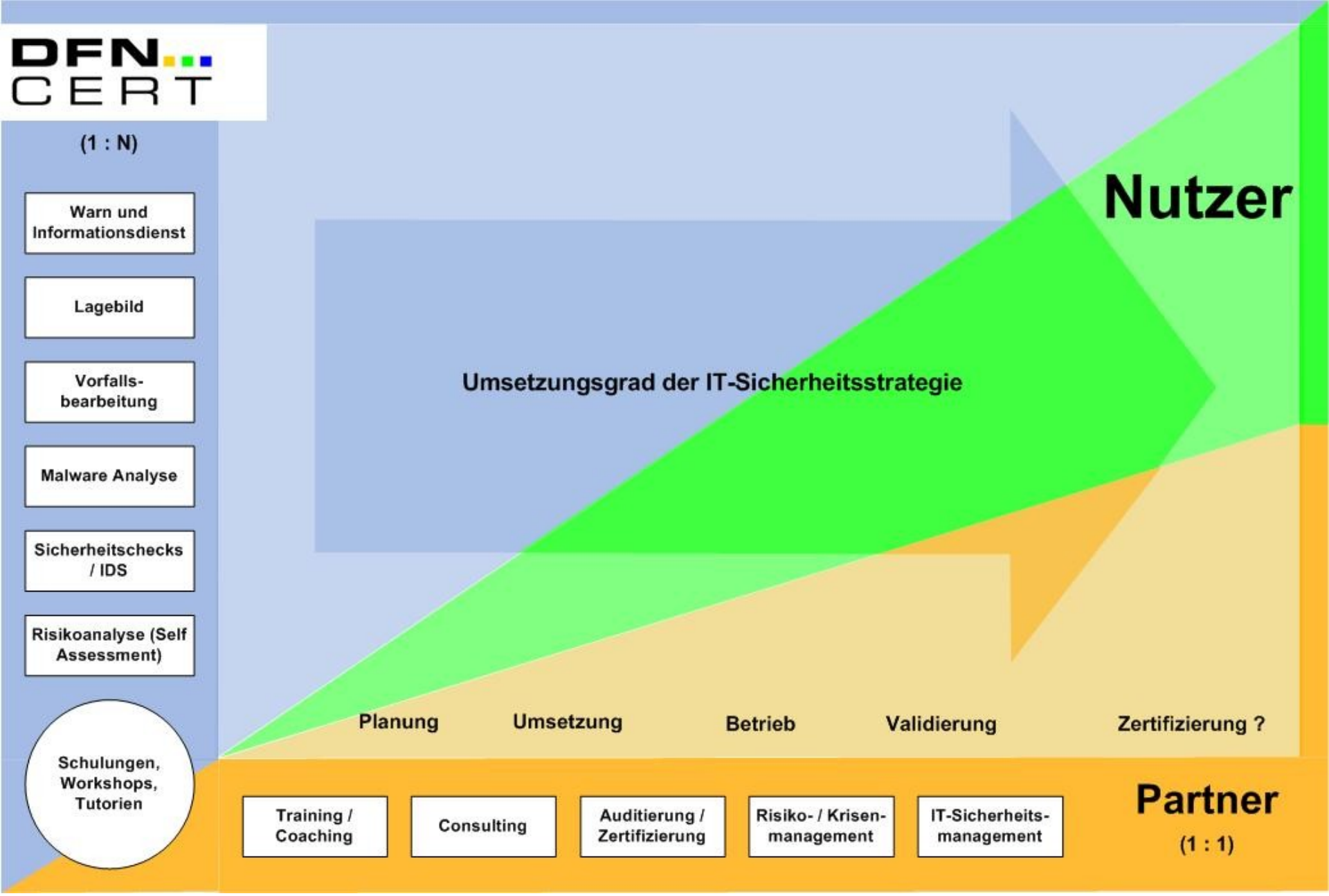


Wer sind wir ?

- DFN-CERT Services GmbH
  - 1993 bis 1999 als Projekt an der Uni Hamburg
  - Kunde: DFN-Verein
  - Betreute Klientel: Anwender des DFN-Vereins
- Organisationsstruktur
  - Computer-Notfallteam
  - PKI Team
  - Projekt- und Entwicklungsteam
  - Infrastrukturteam
- Veranstaltungen
  - Jährlicher DFN-Workshop „Sicherheit in vernetzten Systemen“
  - Tutorien und Schulungen

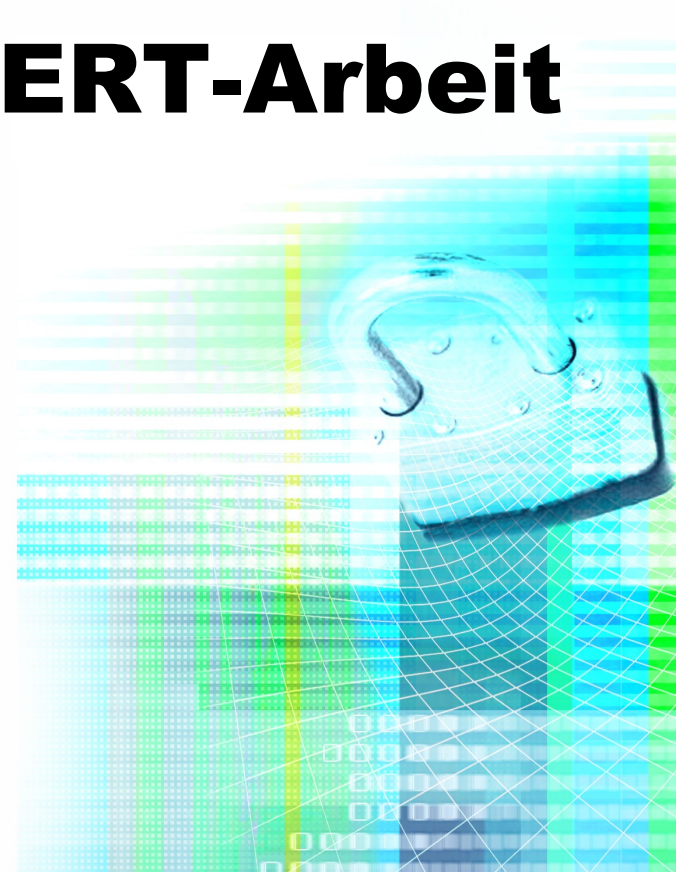
Aufwand & Nutzen




DFN CERT
(1 : N)
Warn und Informationsdienst
Lagebild
Vorfalls-bearbeitung
Malware Analyse
Sicherheitschecks / IDS
Risikoanalyse (Self Assessment)
Schulungen, Workshops, Tutorien
Nutzer
Umsetzungsgrad der IT-Sicherheitsstrategie
Planung
Umsetzung
Betrieb
Validierung
Zertifizierung ?
Training / Coaching
Consulting
Auditierung / Zertifizierung
Risiko- / Krisen-management
IT-Sicherheits-management
Partner
(1 : 1)

DFN CERT

Prävention – eine Säule der CERT-Arbeit

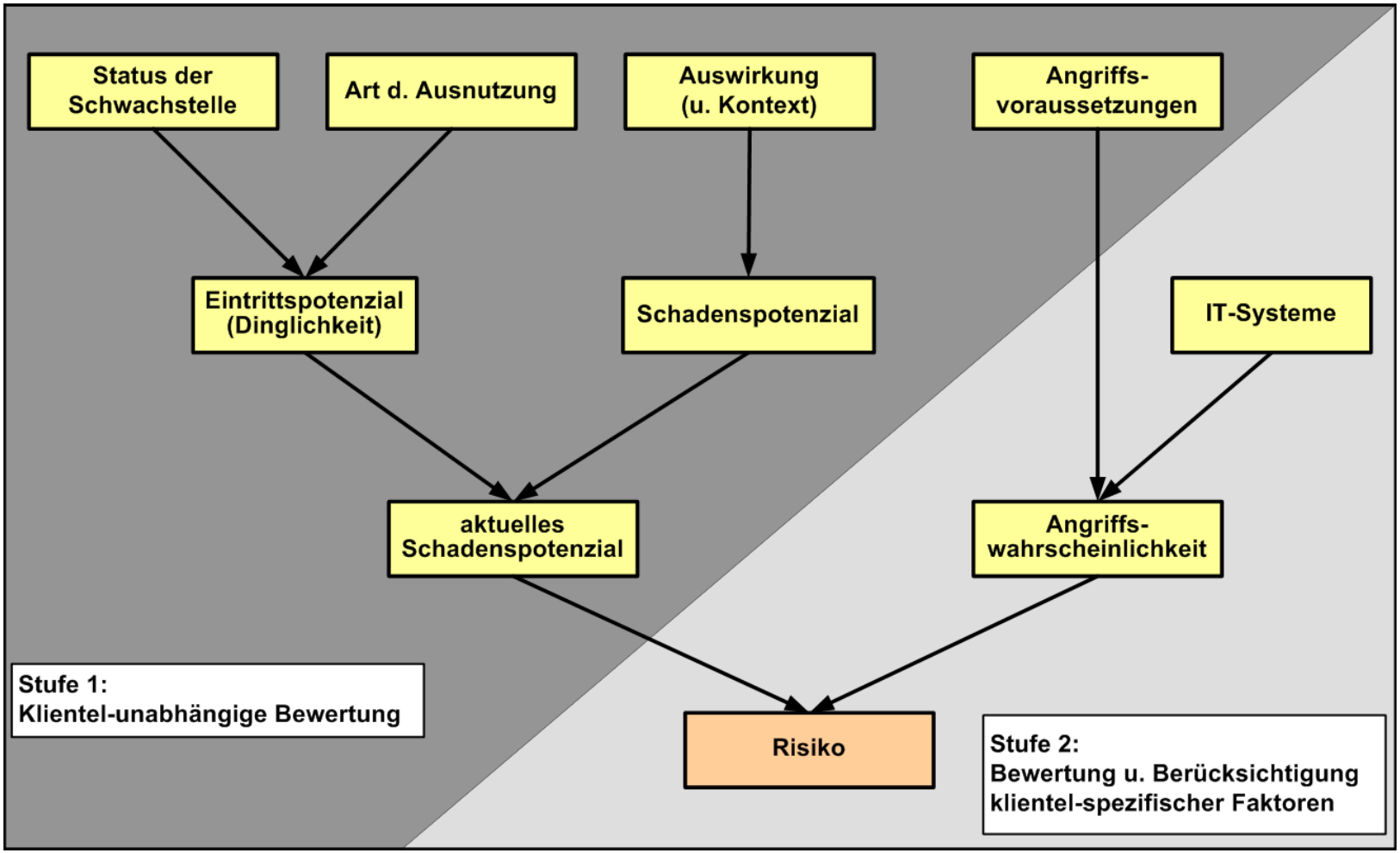


Prävention: Security Advisories

- Grundlage: Deutsches Advisory-Format (DAF)
- Einheitliches Format für Erstellung und Austausch von Sicherheits-Advisories
- Entwickelt und gepflegt von
  - CERT-BUND (BSI), DFN-CERT, Siemens CERT und PRESECURE
- XML-Format basierend auf EISPP (www.eispp.org)
- Mittelpunkt: eine Schwachstelle in einer Software oder Hardware
- Inzwischen als frei konfigurierbares Kundenportal („massgeschneiderte“ Advisories und selbst definierte Verteilungswege)

Prävention: Security Advisories

DAF: Klassifizierungsschema für Schwachstellen



Prävention: Security Advisories

DFN CERT

DAF: Ermittlung des potentiellen Schadens

Schadenspotenzial

Schadenspotenzial	Kontext			
Verlust	Benutzer	Dienst	System	Netzwerk
Übernahme der Kontrolle	hoch	hoch	sehr hoch	sehr hoch
Übernahme von Berechtigungen	mittel	mittel	hoch	hoch
Integrität	gering	mittel	hoch	hoch
Vertraulichkeit	sehr gering	gering	mittel	hoch
Verfügbarkeit	sehr gering	gering	mittel	hoch
Umgehung von Sicherheitsmaßnahmen	sehr gering	gering	mittel	hoch

Prävention: Security Advisories

Plattform Categorisation	Windows, Windows 95/98/ME, Windows NT, Windows 2000, Windows XP, Windows Server 2003

Plattform Description

Microsoft Windows NT Server 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
Microsoft Windows 2000 Service Pack 3 und 4
Microsoft Windows XP, Microsoft Windows XP Service Pack 1 und 2
Microsoft Windows XP 64-Bit Edition Service Pack 1
Microsoft Windows XP 64-Bit Edition Version 2003
Microsoft Windows Server 2003
Microsoft Windows Server 2003 64-Bit Edition
Microsoft Windows 98,
Microsoft Windows 98 Second Edition (SE)
Microsoft Windows Millennium Edition (Me)

Software Categorisation	Client

Software Description

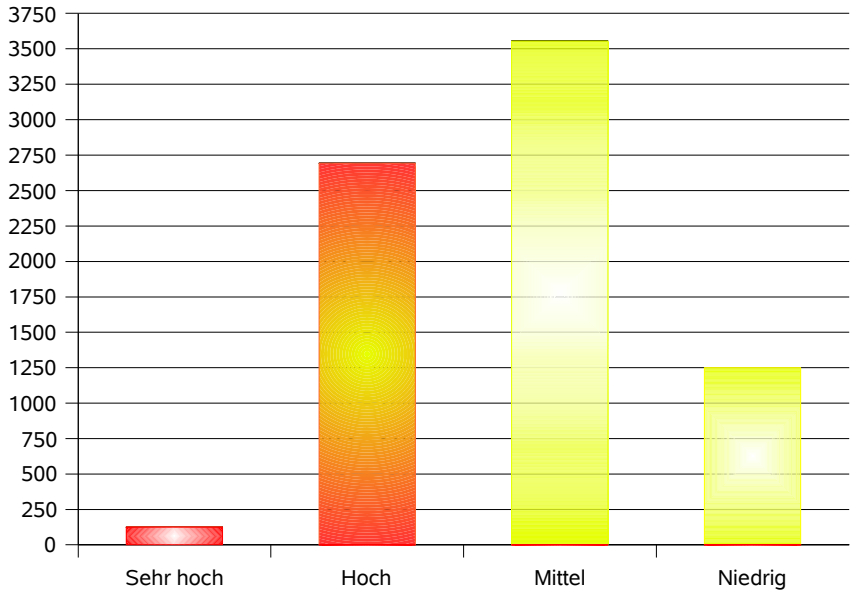
Internet Explorer 5.01, 5.5 und 6

Vulnerabilities

Status	Exploit published
Propagation	Automated
Scope and Loss	Code Execution as Admin (very high impact)
Requirements	Victim interaction: access content
Categorisation	Buffer Overflow, Heap Overflow, Cross-site Scripting
Immediacy	High (Proposal: High)
Current Impact	Very high (Proposal: Very high)

Bisherige Advisories

object	no. of instances in DB
EISPP advisories	7654
vendor (aka original) advisories	9036
different vulnerabilities	5791
solution sections	7940
referenzes	36092
uris	36649



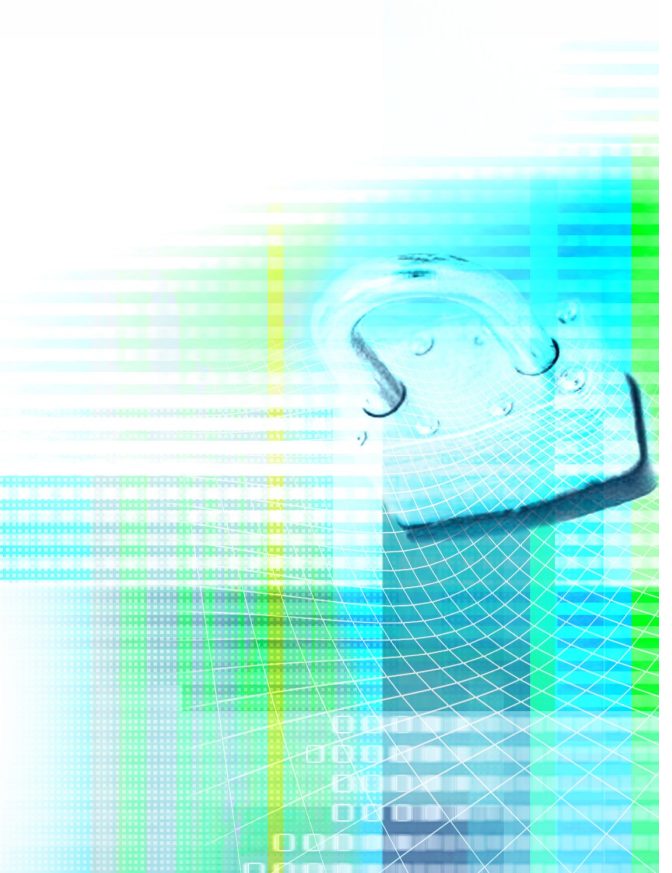
category	all adv.
Buffer Overflow	2276
Integer Overflow	1025
Heap Overflow	964
Design Schwaeche	791
Cross-site Scripting	750
Race Condition	523
Null Pointer Referenzierung	370
Fehlerhafte Array-Indizierung	287
Ungepruefte Uebernahme von Variablen	277
Format String Fehler	253
Speicherleck	197
Unsichere Fehlerbehandlung	176
Double Free Fehler	151
Quoting Fehler	149
Fehler durch temporaere Dateien	140
Directory Traversal Schwachstelle	136
Nicht initialisierter Speicher	116
Unsichere Default-Konfiguration	113
SQL Injection	92

Was machen Sie?

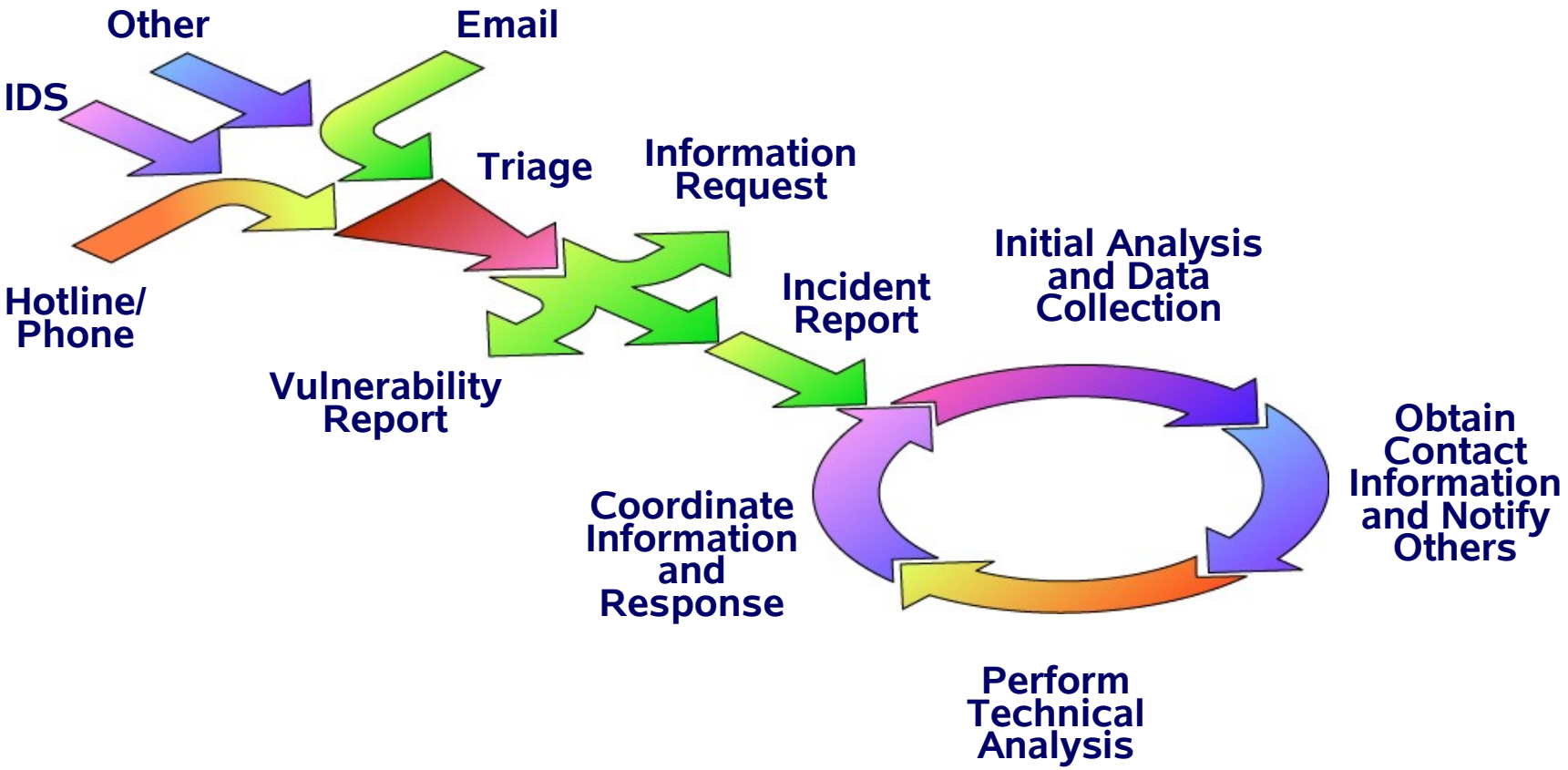
- in Bezug auf die aktuelle Absicherung der Systeme

DFN CERT

Reaktion – die zweite Säule der CERT-Arbeit



Betreuung und Reaktion



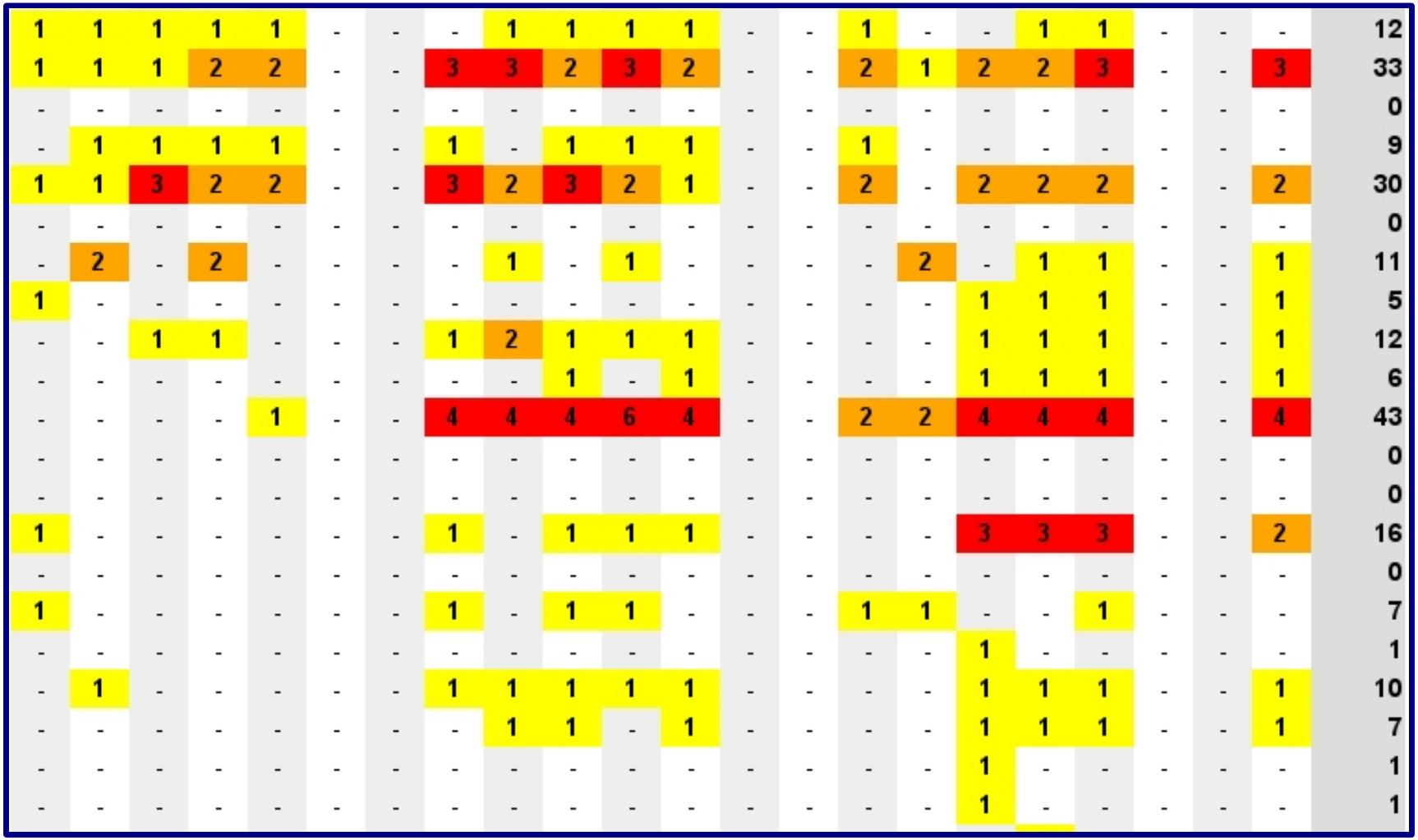
Aufgaben des Experten

- Entgegennahme von Berichten und Meldungen
- Analyse von Vorfallsmeldungen
- Analyse von Vorfallsmaterial (Logfiles, Artefakte, etc.)
- Recherche nach Ansprechpartnern
- Koordination und Verteilen von Informationen
- Zusammenarbeit mit anderen Teams, Einrichtungen, etc.
- Technische Unterstützung, allerdings in unterschiedlichen Ausprägungen:
  - am Telefon, per E-Mail
  - vor Ort als Teil der weiteren Arbeitsaufgaben
  - vor Ort als kostenpflichtige Zusatzdienstleistung

Was wird gemeldet?

- Einrichtung meldet kompromittierter Server mit sichergestelltem Material (Artefakte)
- Anderes CERT berichtet von einem kompromittierten System im Verantwortungsbereich
- Portscan-Meldungen (automatisiert und manuell)
- Viren- und Proxy-Meldungen (meist automatisiert)
- Infizierte Benutzersysteme
- Anfragen von Strafverfolgungsbehörden
- De-Facements
- ...

Aktuelle Warnungen



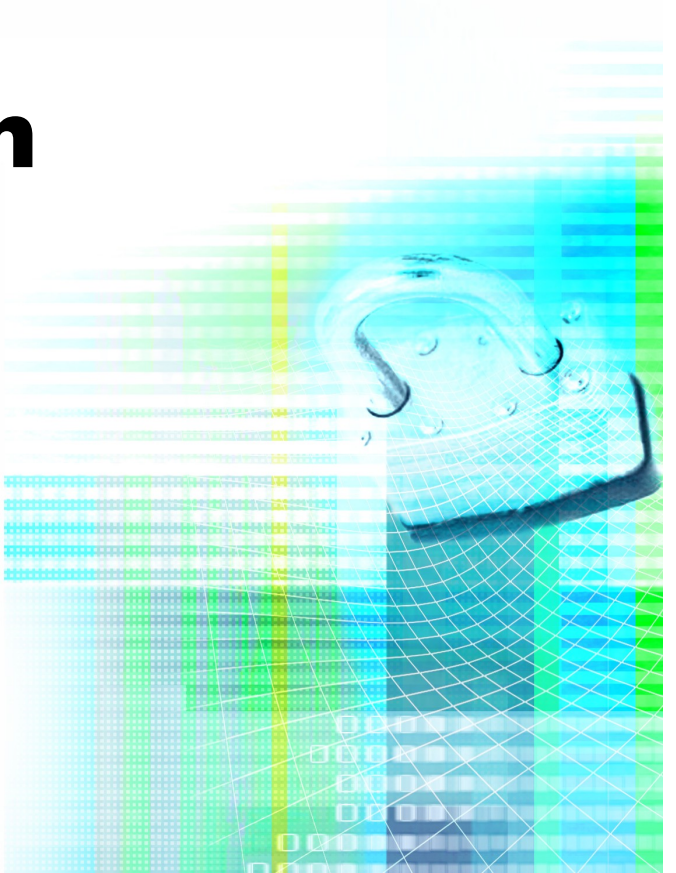
1	1	1	1	1	-	-	-	1	1	1	1	-	-	1	-	-	1	1	-	-	-	12
1	1	1	2	2	-	-	3	3	2	3	2	-	-	2	1	2	2	3	-	-	3	33
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
-	1	1	1	1	-	-	1	-	1	1	1	-	-	1	-	-	-	-	-	-	-	9
1	1	3	2	2	-	-	3	2	3	2	1	-	-	2	-	2	2	2	-	-	2	30
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
-	2	-	2	-	-	-	-	1	-	1	-	-	-	-	2	-	1	1	-	-	1	11
1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	1	1	-	-	1	5
-	-	1	1	-	-	-	1	2	1	1	1	-	-	-	-	1	1	1	-	-	1	12
-	-	-	-	-	-	-	-	-	1	-	1	-	-	-	-	1	1	1	-	-	1	6
-	-	-	-	1	-	-	4	4	4	6	4	-	-	2	2	4	4	4	-	-	4	43
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
1	-	-	-	-	-	-	1	-	1	1	1	-	-	-	-	3	3	3	-	-	2	16
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0
1	-	-	-	-	-	-	1	-	1	1	-	-	-	1	1	-	-	1	-	-	-	7
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1
-	1	-	-	-	-	-	1	1	1	1	1	-	-	-	-	1	1	1	-	-	1	10
-	-	-	-	-	-	-	-	1	1	-	1	-	-	-	-	1	1	1	-	-	1	7
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	1

Was machen Sie?

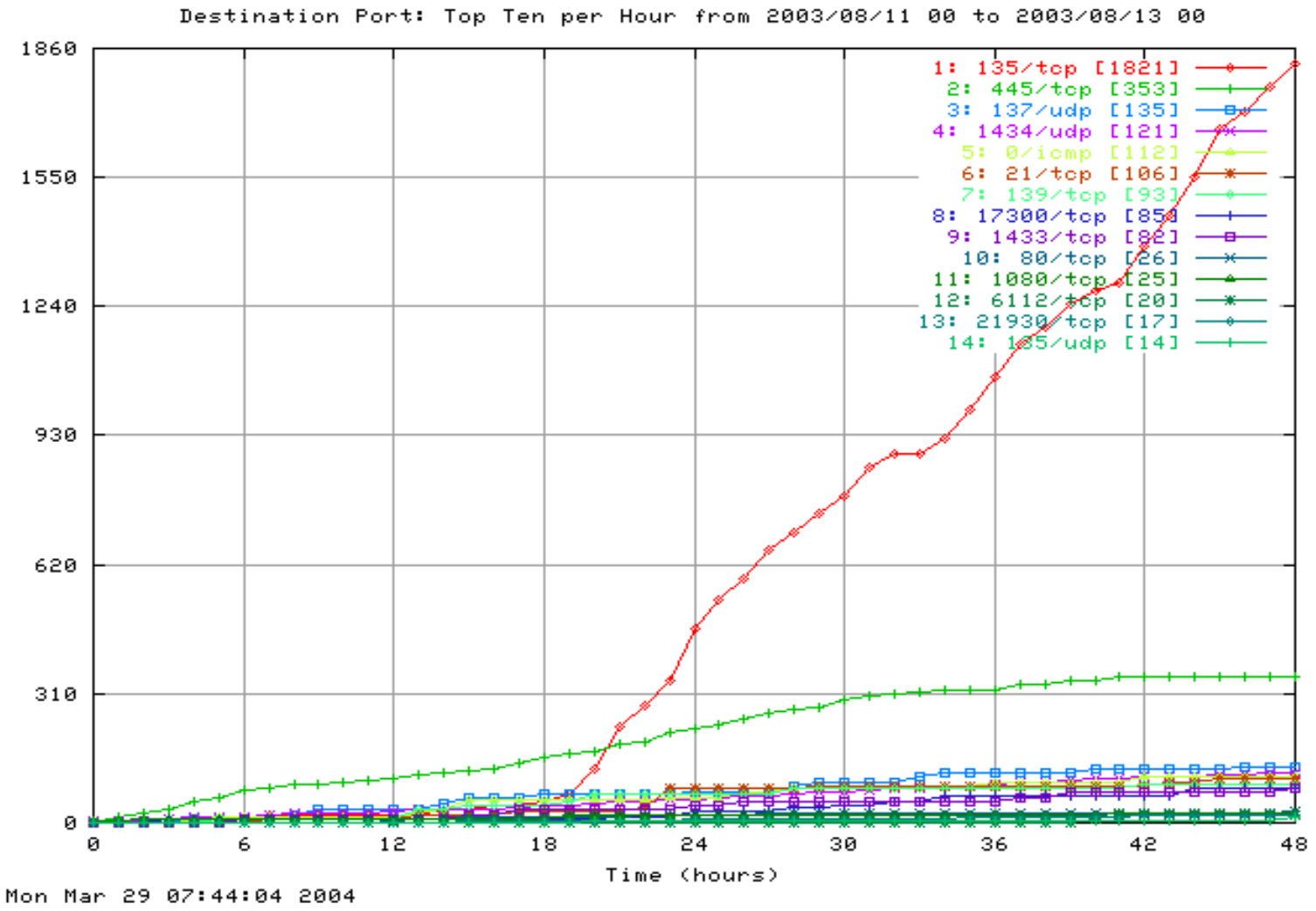
- in Bezug auf die Vorfallsbearbeitung

DFN CERT

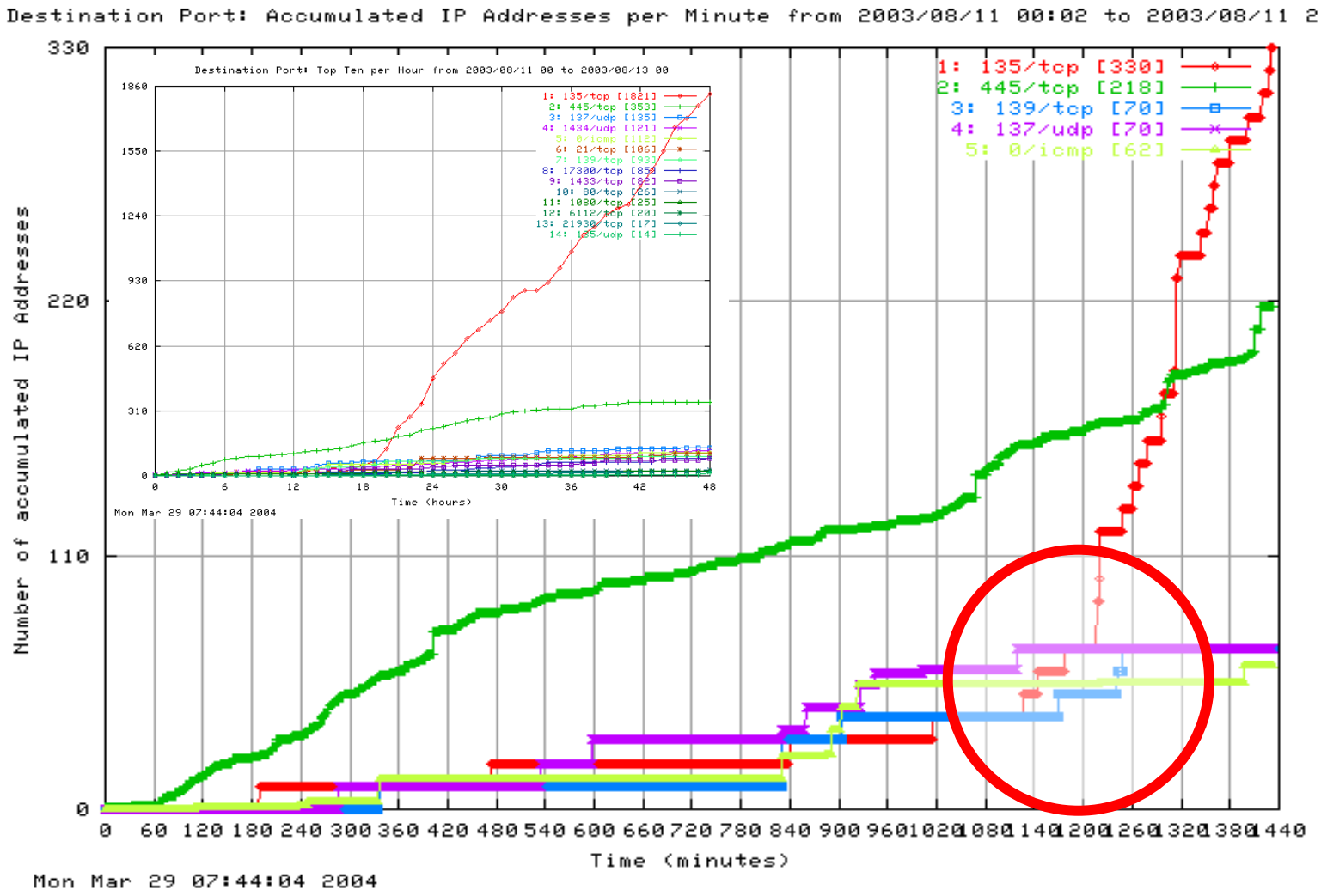
Erkennung von Bedrohungslagen und Trends



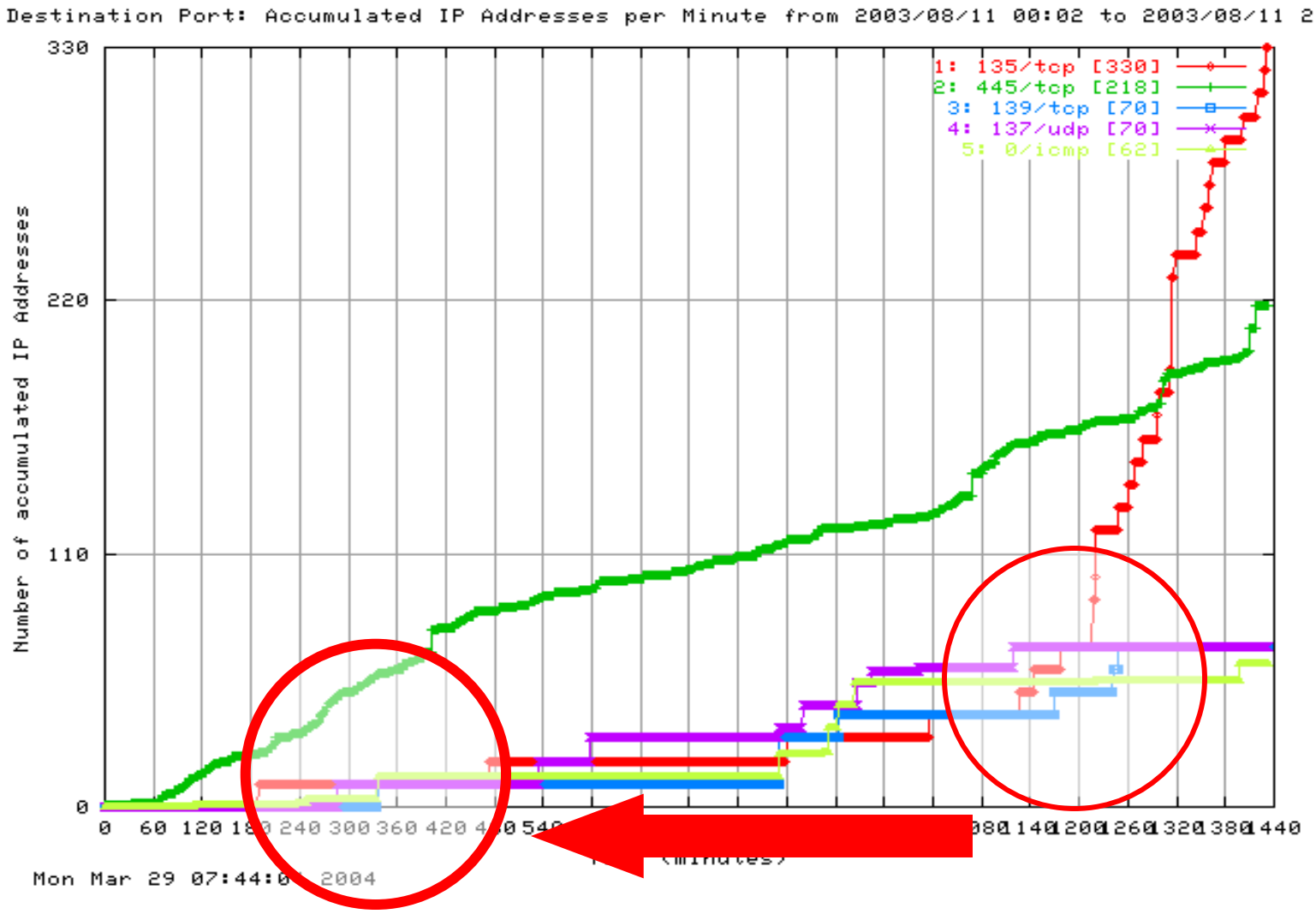
Beispiel August 2003: Blaster



Die Stunde der Wahrheit



Die Stunde der Wahrheit



Microsoft RPC [MS08-067]

- 23. Oktober 2008
  - Remote Exploit:
    - Windows 2000 *)
    - Windows XP *)
    - Windows VISTA
    - Windows Server 2003 *)
    - Windows Server 2007
    - Windows 7 beta
  - *) ohne vorherige Authentisierung
  - Präparierte RPC-Requests besitzen konkretes Potential für neuen Wurm

Originalfolie vom 11. November 2008

Microsoft RPC [MS08-067] (2)

- 25. Oktober 2008
  - Öffentlich verfügbarer Exploit-Code
  - Gestiegene Aktivitäten im gesamten Internet
  - Wurm Gimmiv.A wird im Internet gefunden
    - Erste Signaturen für Viren-Scanner und IDS
    - Allerdings kein Wurm, sondern Trojaner, welcher bisher die automatische Ausbreitung unterließ
  - Windows Firewall nur bedingter Schutz
    - Datei- und Druckerfreigabe schaltet Ports frei!
  - XP und Server 2003 kein Schutz
    - Dateiausführungsverhinderung nicht aktiviert!

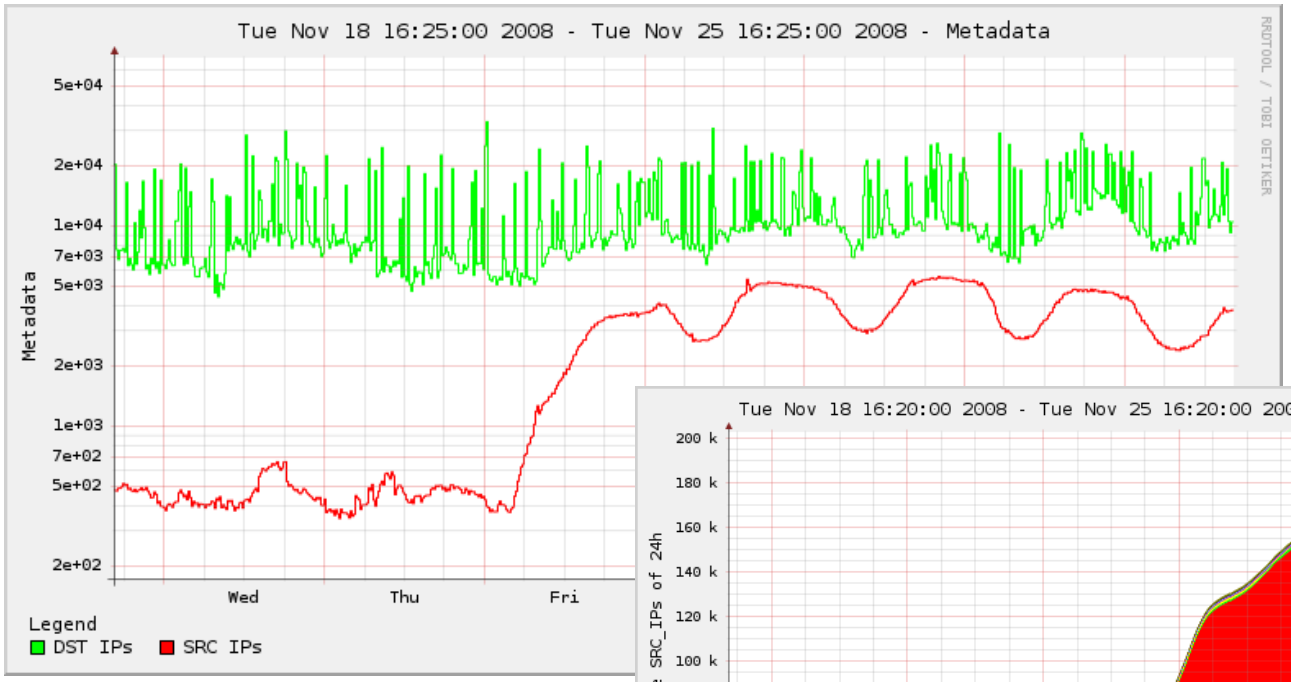
Originalfolie vom 4. November 2008

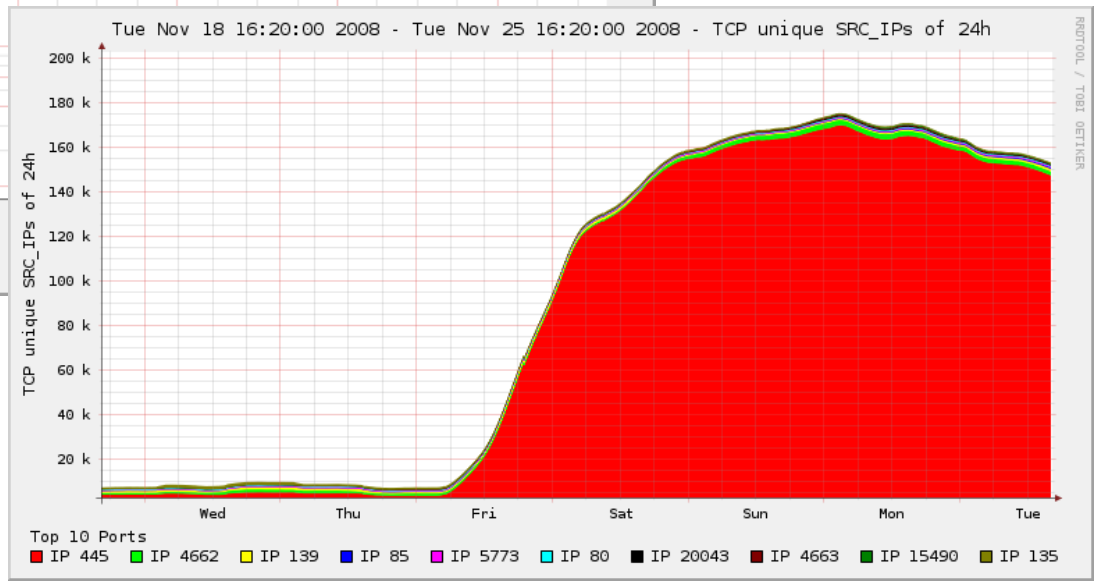
Conficker

- 14. November 2008
  - Microsoft meldet, dass 50 verschiedene Exploits identifiziert wurden, die die Schwachstelle ausnutzen.
  - Kommerzielles Angriffswerkzeug kann in China gekauft werden.
- Es dauert jedoch noch eine Woche bis zur ...

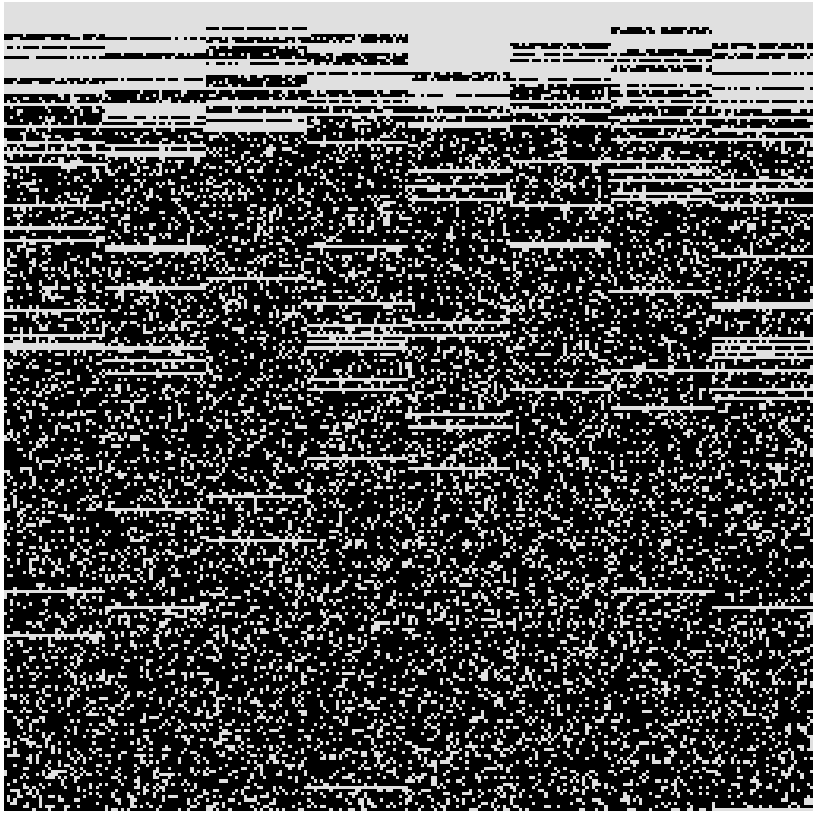
... ersten Angriffswelle

- CarmentiS alarmiert frühzeitig!





Conficker ist berechenbar

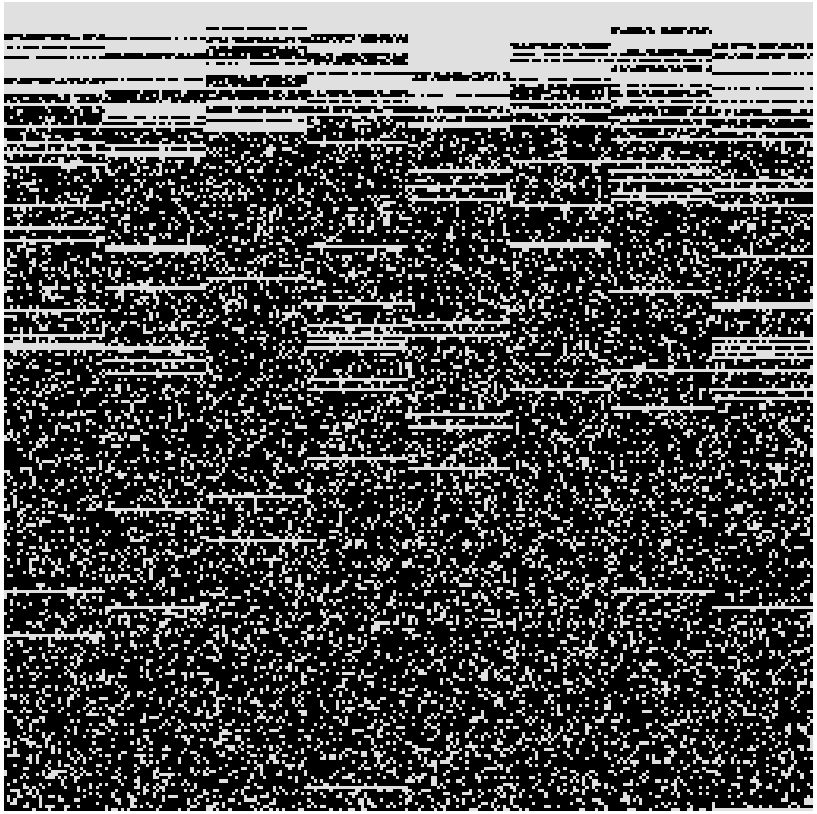


➲ *Algorithmen von Conficker zeigt deutliche Muster bei den genutzten TCP-Ports*

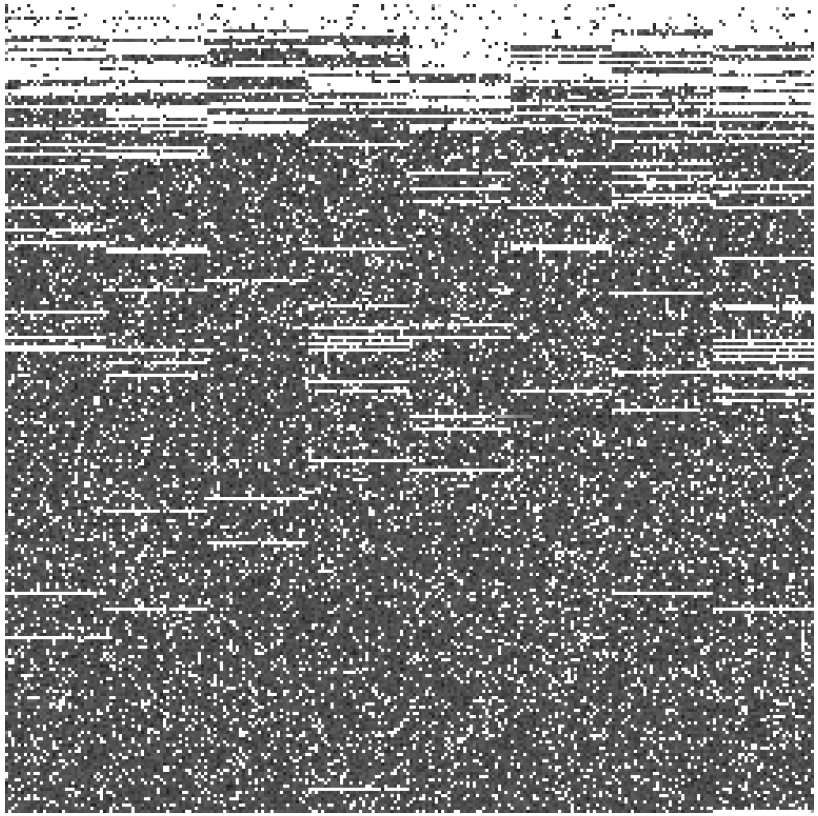
Conficker dominiert Angriffsverkehr

DFN CERT

Theorie



Praxis im Juli 2009

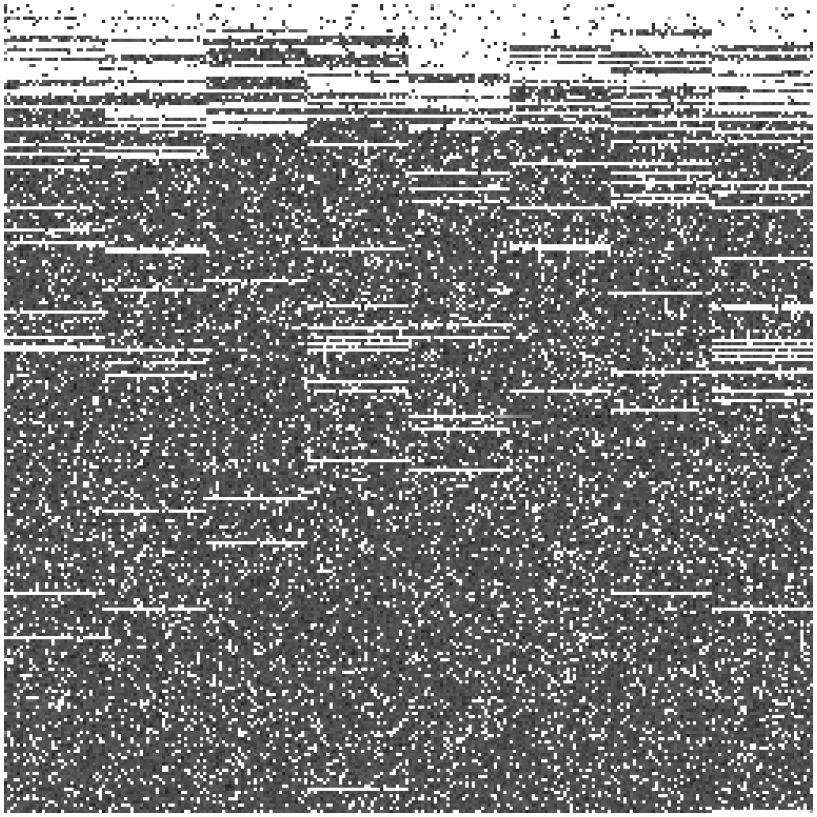


➲ *Frühwarnsystem zeigt uns deutlich dieses Muster!*

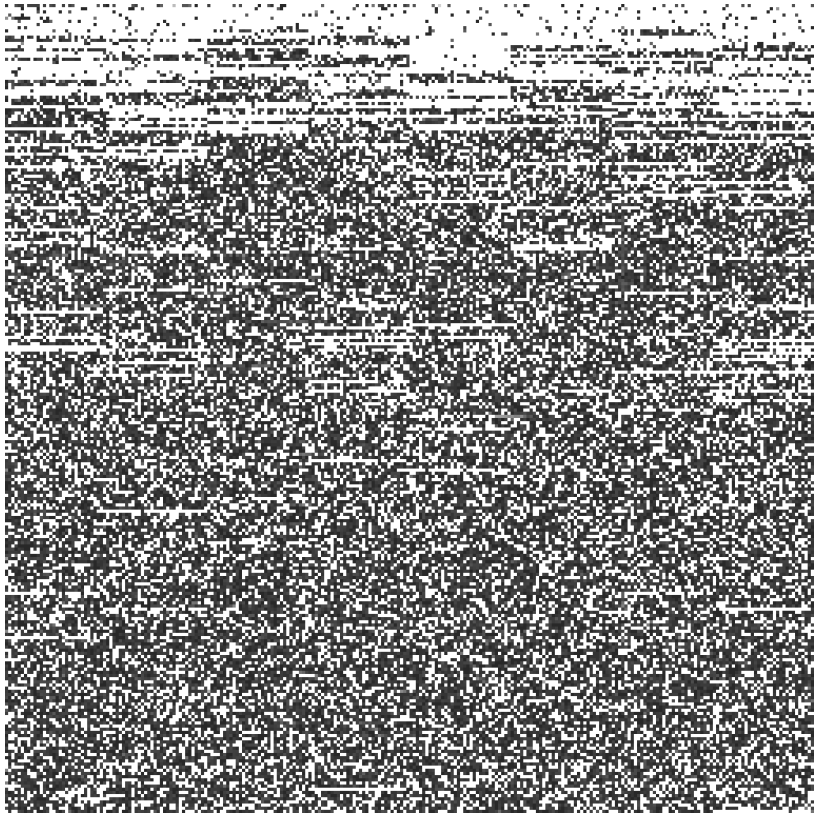
Conficker dominiert Angriffsverkehr

DFN CERT

Praxis im Juli 2009



und im Oktober 2009



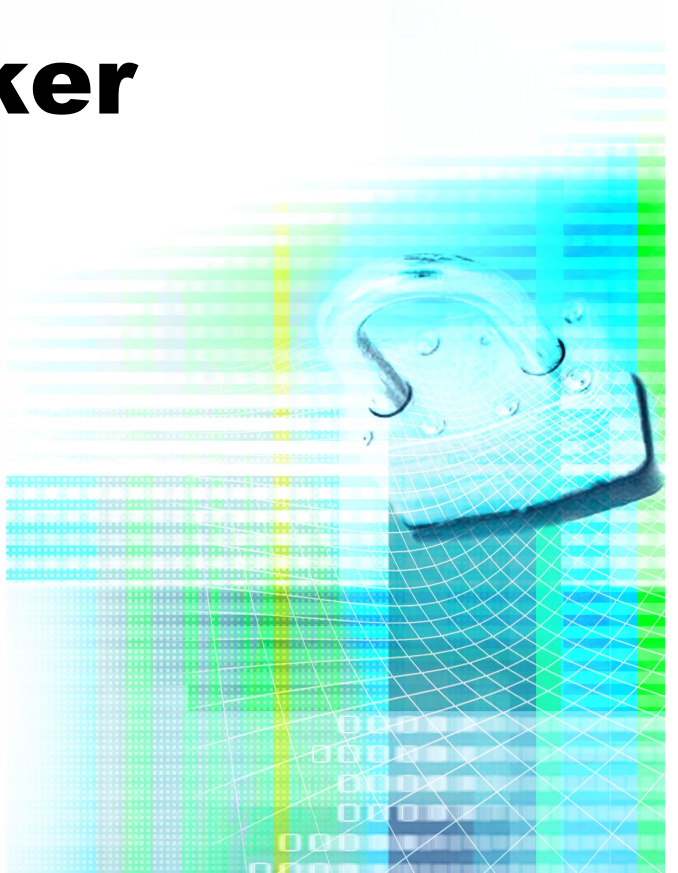
➲ ***Matrix zeigt das Muster nur noch abgeschwächt!***

Was machen Sie?

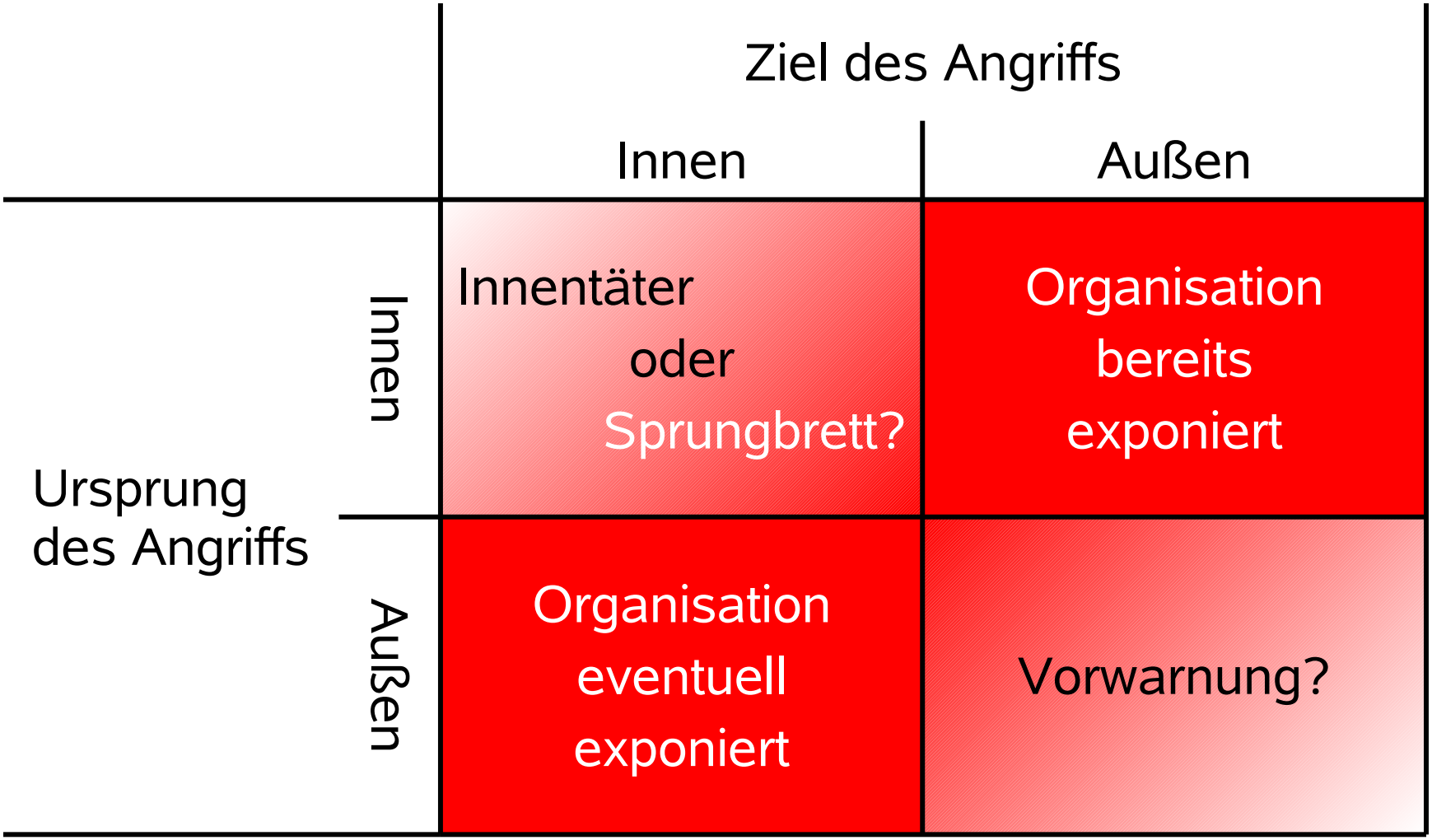
- in Bezug auf die Bewertung der Lage

DFN CERT

... im Verbund sind CERTs stärker



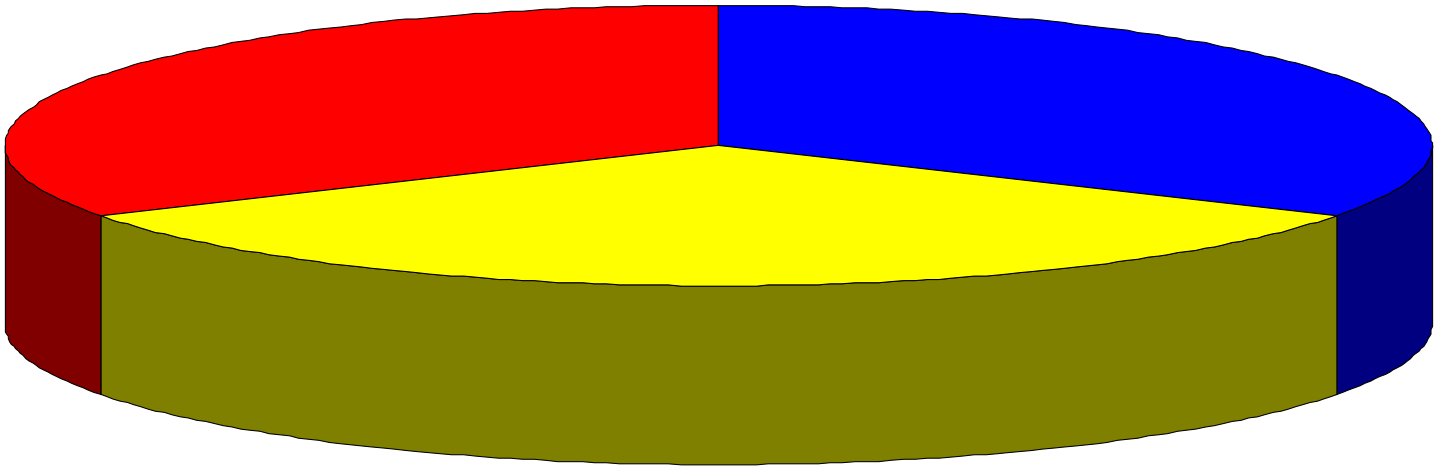
Vorfälle gibt es!



Vorfallsberichte

andere CERTs
~ 33,3%

andere Betroffene
~ 33,3%



die eigene Constituency
~ 33,3%

CERT im nationalen Verbund

- **Nationaler CERT-Verbund**
  www.cert-verbund.de
  - Allianz deutscher Sicherheits- / Computernotfallteams

CERT-BUND (BSI)
DFN-CERT
IBM BCRS
S-CERT (SIZ Sparkassen)
Siemens-CERT
Telekom-CERT
PRESECURE
RUS-CERT (Uni Stuttgart)
CERTBw (Bundeswehr)
COMCert (Commerzbank)
CERT-VW (Volkswagen)

… in Europa und Global

- **FIRST (www.first.org)**
  - Weltweiter Dachverband
  - Zusammenarbeit auf technischer Ebene

- **TERENA TF-CSIRT (www.terena.nl)**
  - Europaweite Arbeitsgruppe
  - Zusammenarbeit auf technischer und konzeptioneller Ebene; Kontakte zur EU
  - Trusted Introducer (TI, nächste Folie)
  - IODEF (jetzt IETF Working Group)
  - Erweiterung der RIPE-Datenbank: IRT Objekt
  - CHIHT: Sammlung von Informationen zu Security Tools

Akkreditierung für CERTs

- **Trusted Introducer TI www.trusted-introducer.org**
  - Ziel: Objektive und aktuelle Informationen über Notfallteams
  - Ermöglicht es neuen (und etablierten) Teams, sich in einer Weise zu präsentieren, die anderen Teams das Auffinden der Informationen erleichtert.
- Unterstützung der Kommunikation und Erleichterung der Zusammenarbeit
- Überprüft durch das TI Review Board
  - verfügt über Sanktionsmöglichkeiten
- Akkreditierung erprobt,
  - Zertifizierung in der Vorbereitung

Zusammenarbeit ja, aber ...

- Keine globalen Aussagen über Folgen
  - Art und Verteilung der Vorfälle
  - Bedrohte bzw. betroffene Werte, Schäden
  - Anzahl und Art der Betroffenen
- Keine globalen Aussagen über Kennzahlen
  - Zeitpunkte und Bearbeitungsdauer
  - Anzahl der Falschmeldungen
  - Anzahl der nicht bearbeiteten Vorfälle

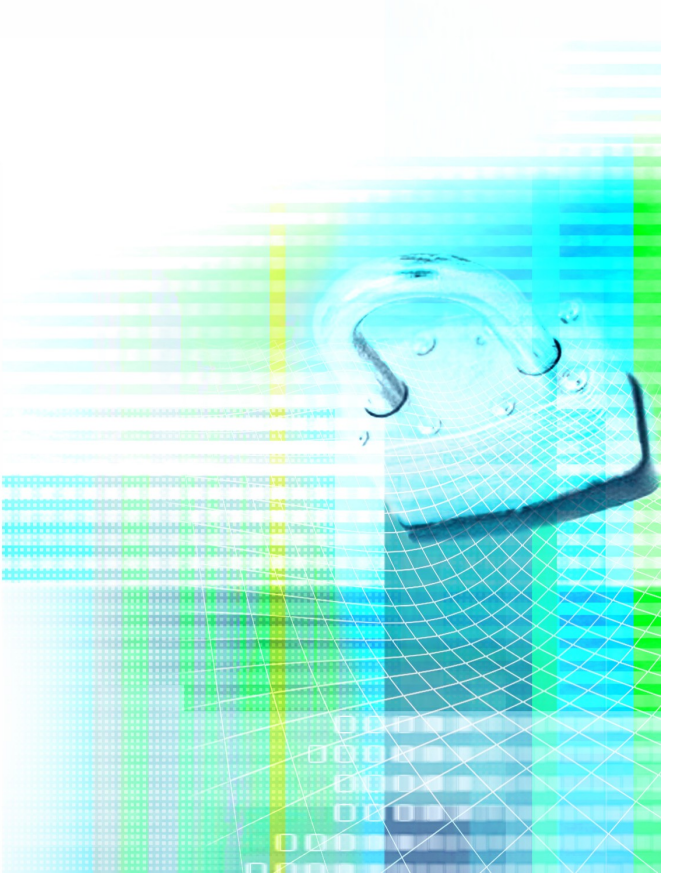
➲ *... ist also unzureichend!*

Was machen Sie?

- ... in Bezug auf die externe Zusammenarbeit

DFN CERT

... brauchen Sie ein CERT?

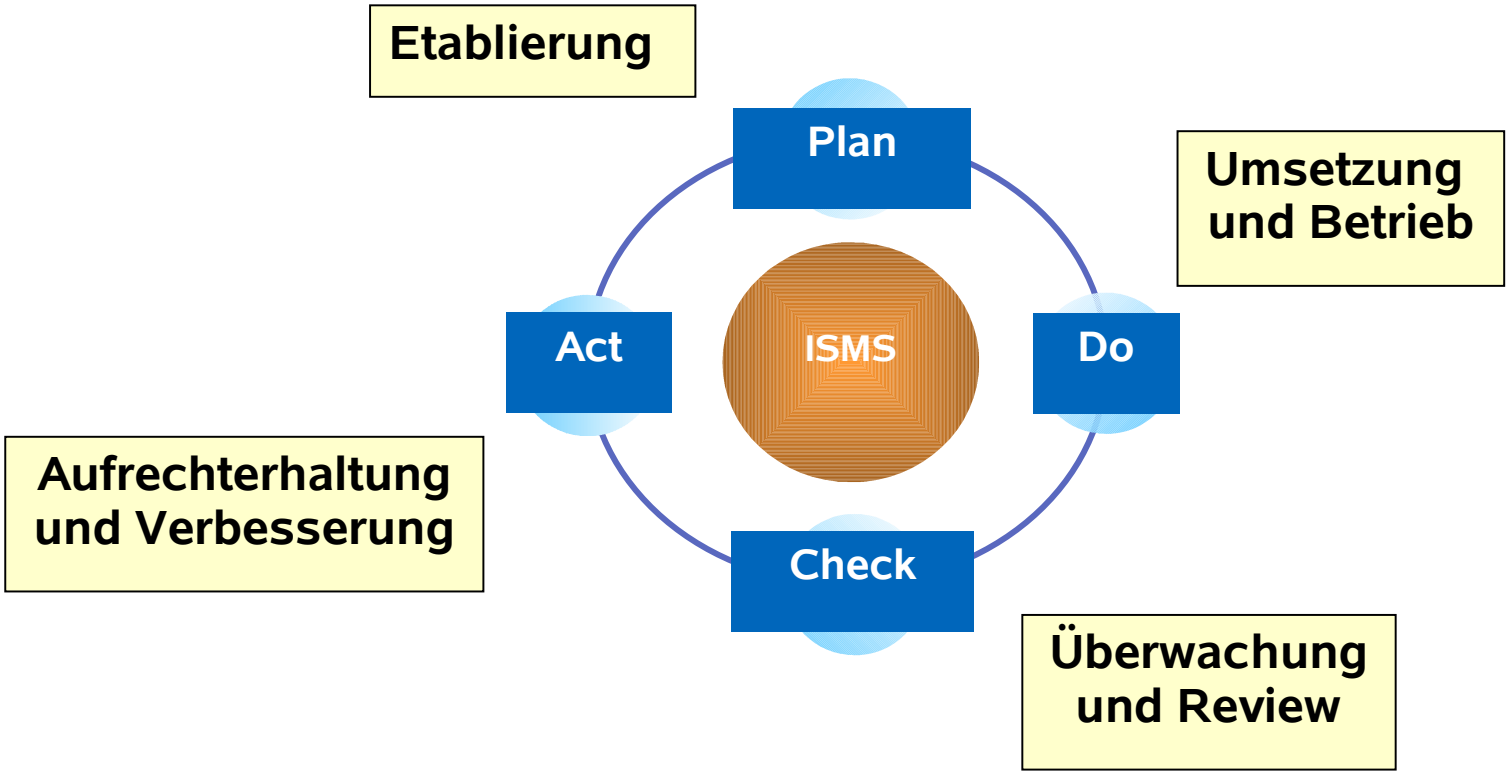


Bekannte Prototypen

- Im Unternehmen
  - Internes Sicherheitsteam
  - Internes Computer-Notfallteam
- Außerhalb des Unternehmens
  - Koordinierendes Computer-Notfallteam
    - Eine eingrenzbare Anwendergruppen
    - Eine Nation
  - Geschäftsmodelle
    - Dienstleister
    - Hersteller

Management von Sicherheit

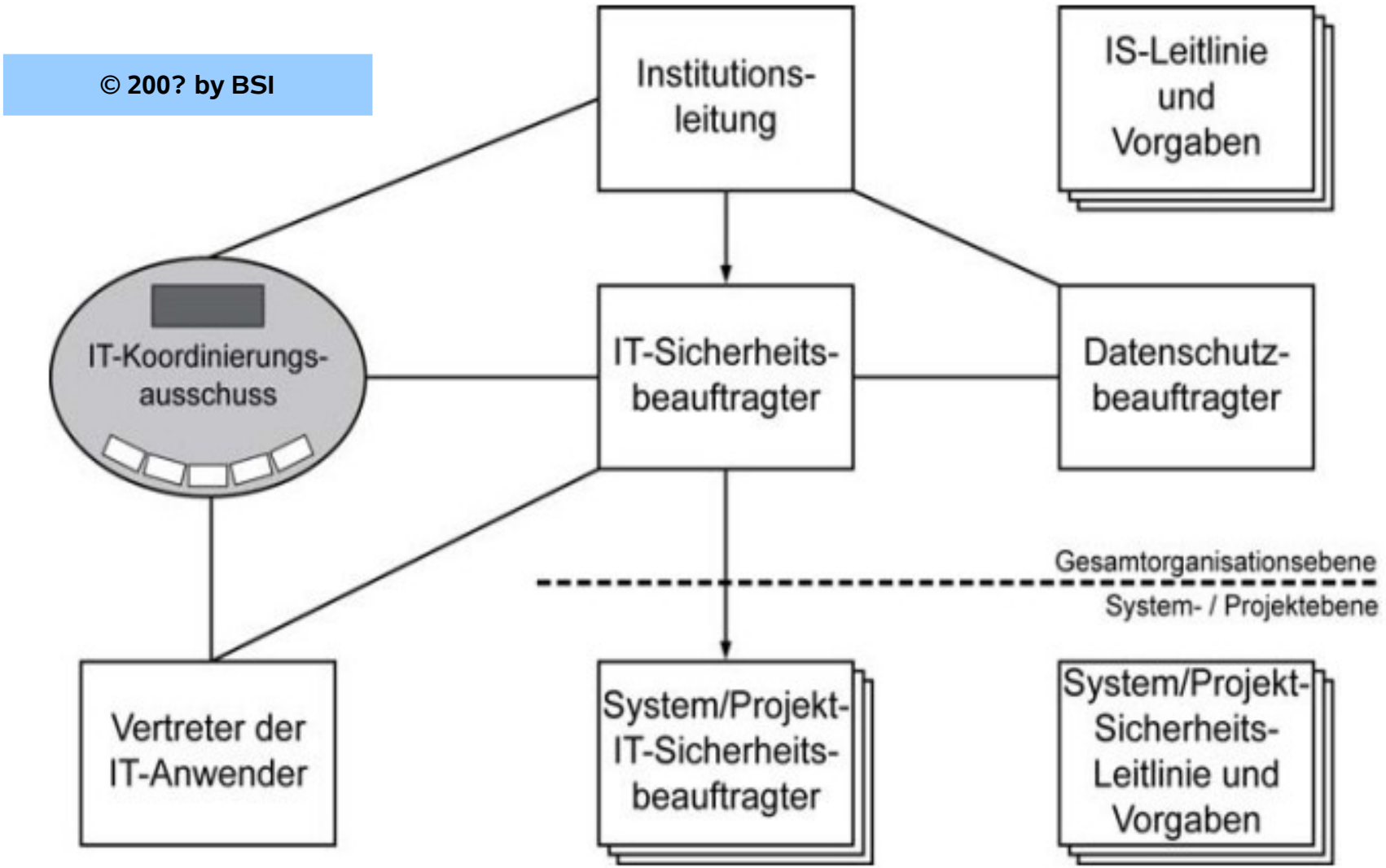
- **Etablierung und Aufrechterhaltung eines Managements als Prozess! (ISMS)**



Aufgaben !?!

- Übernahme der **Gesamtverantwortung** für IT-Sicherheit durch die Leitungsebene
  - Festlegung des **Geltungsbereichs**
  - **Anforderungsanalyse** und –bewertung
  - Ableitung sinnvoller **Ziele** und **Vorgaben**
  - Definition einer **Strategie**
- Definition einer geeigneten **Organisation**, mit Rollen und Verantwortlichkeiten

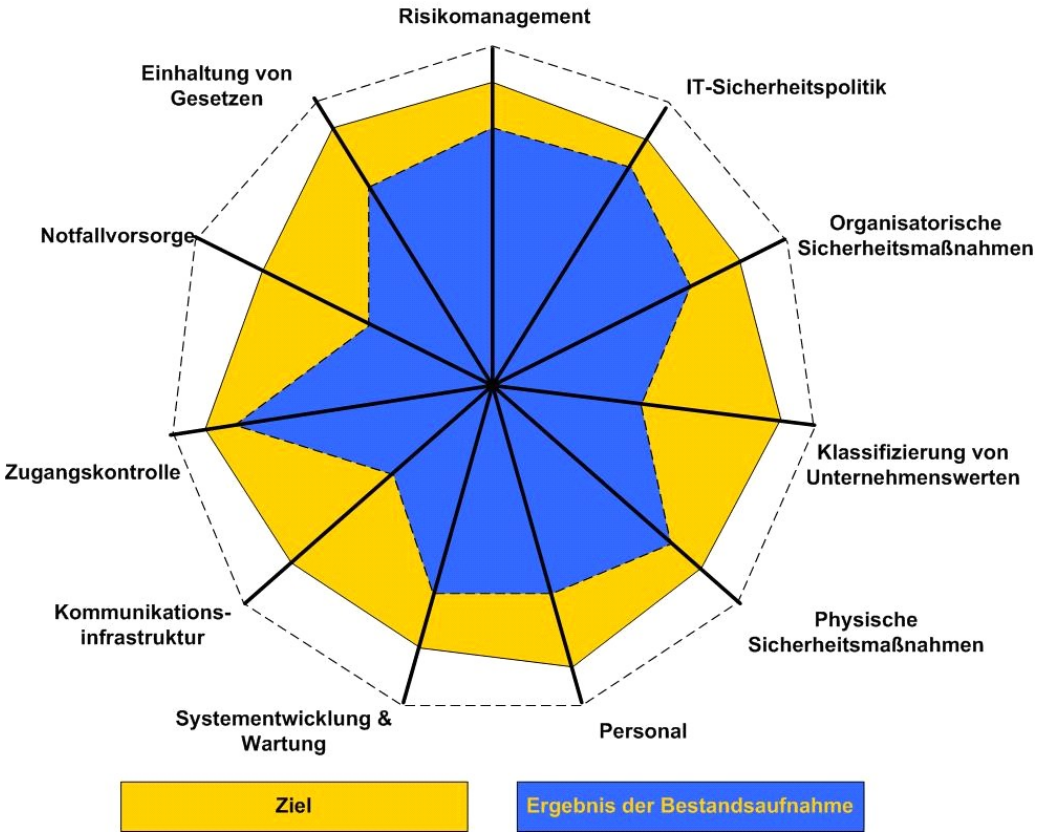
Aufbau für KMUs ?!?



IT-Sicherheitsmanagement

- **Risikoanalyse**
  - Self Assessment
  - Checklisten
  - Fragebögen
  - Optional - Kick-Off und Evaluierung durch Experten
- **Ergebnisse**
  - Strategische u. taktische Vorgaben für die
  - Themenbereiche nach BSI 7799 bzw. ISO 27001

OCTACE Methodik



Rolle der Incident Response

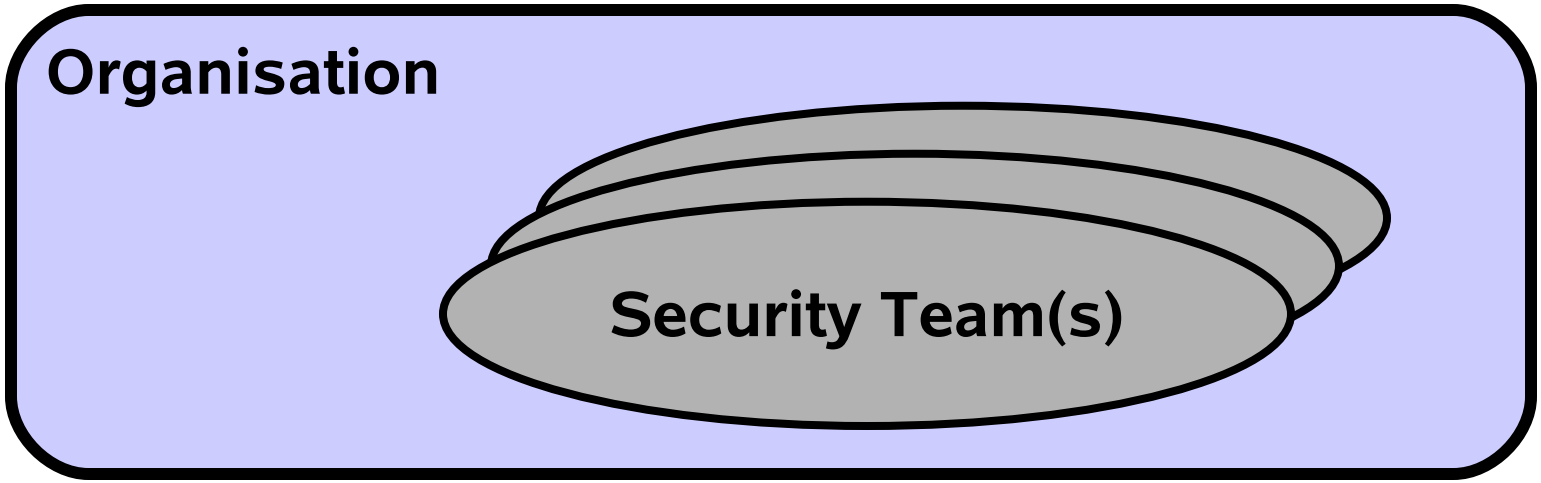
- Gehört zum Risiko- / Sicherheitsmanagement
- Ist eine Vermittlungsinstanz zwischen:
  - Systemadministratoren und Management
  - und zu externen Organisationen
- Stellt besondere Expertise bereit
  - z. B. Beweissicherung, Kontakte, ...
- Ersetzt keine technischen Maßnahmen
  - z. B. Intrusion Detection Systems

Was haben Sie denn?

- Selbst im Unternehmen
  - Internes Sicherheitsteam
  - Internes Computer-Notfallteam
- von außerhalb des Unternehmens
  - Koordinierendes Computer-Notfallteam
    - Eine eingrenzbare Anwendergruppen
    - Eine Nation
  - Geschäftsmodelle
    - Dienstleister
    - Hersteller

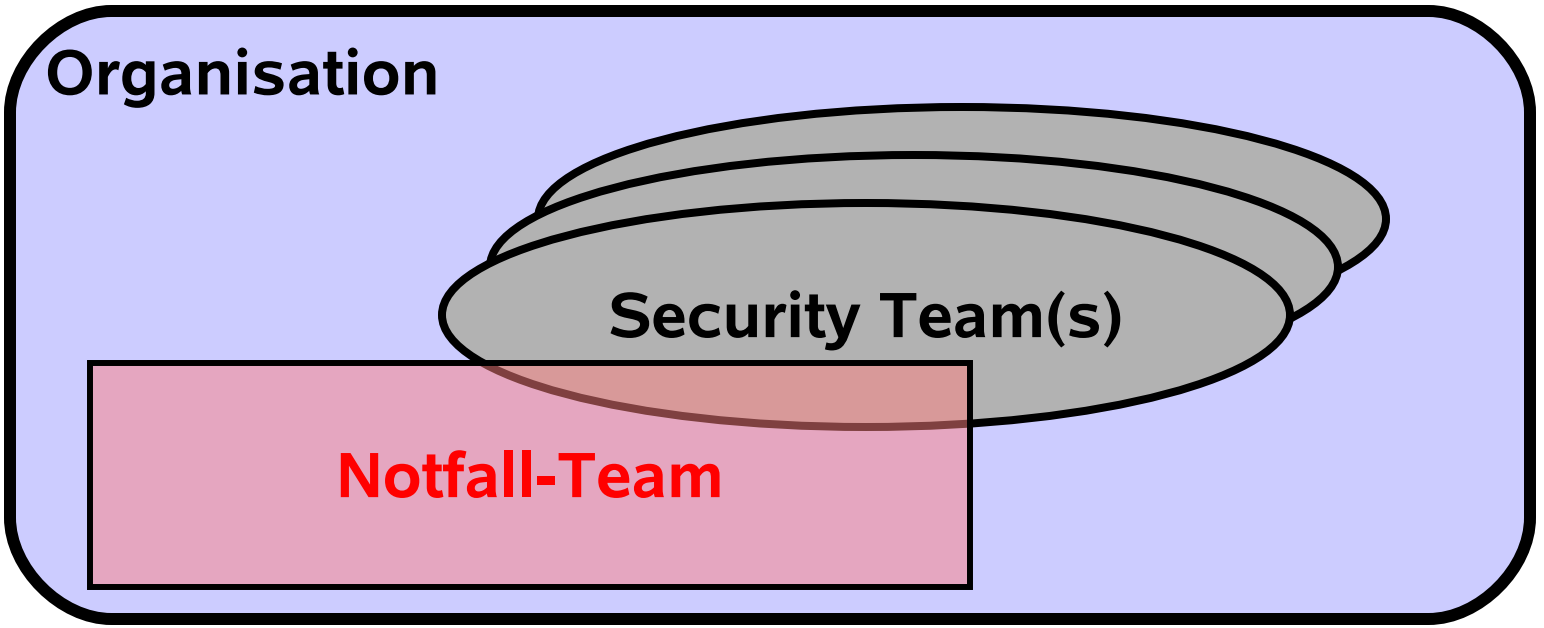
Internes Sicherheitsteam

- Verantwortlich für die Sicherheit der Systeme (Server, Firewalls, Virenfilter, etc.)
- Eventuell mehrere solcher Teams
- Zuständigkeiten klar definiert



Internes Notfallteam

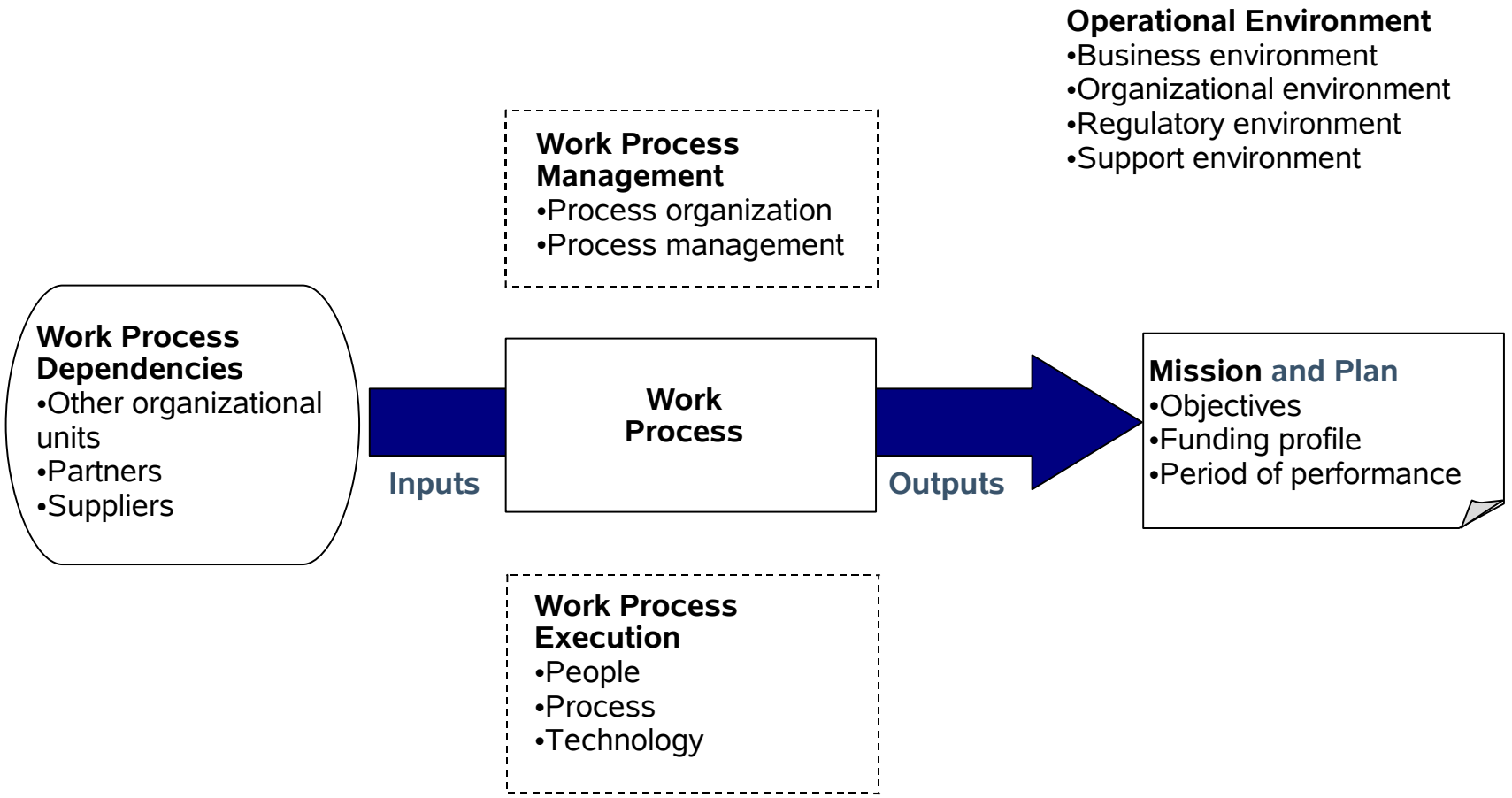
- Spezialisierung von Sicherheitsteams
- Institutionalisierung der Vorfallsbearbeitung



Re-Engineering?

- Gehört ein Sicherheits- / Risikomanagement bereits zur etablierten Kultur?
  - Identifizierung relevanter Geschäftsprozesse
  - Erfassung der heutigen Arbeitsprozesse
  - Re-Engineering der Prozesse
- Die relevanten Prozesse werden angepasst
  - Steigerung von Effizienz und Effektivität
  - Neuausrichtung
  - Verständnis von Stärken und Schwächen
- Neue Schnittstellen zu anderen Prozessen

Prozesse im Mittelpunkt!



Prävention

- Sicherheitsmeldungen (Advisories)
  - Warnungen
  - Alarmierungen
- Trendanalyse (Technology Watch)
- Sicherheitsüberprüfungen (Audits)
- Neighbourhood Watch
- Entwicklung und Einsatz von Sicherheitstools
- Einbruchserkennung und -verhinderung (Intrusion Detection / Prevention)

Reaktion

- Hotline und „Clearinghouse“
- Schwachstellenanalyse, Koordination
- Analyse von Schadsoftware (Malware)
- Forensische Analyse
- Incident Response vor Ort (Resolution)
- Incident Response Support
- Incident Response Koordinierung
- Zusammenarbeit mit anderen Notfallteams

Nachhaltigkeit

- Einbringen der Erfahrungen und Erkenntnisse in das allgemeine Sicherheitsmanagements, z. B.
  - Risiko Analyse
  - Business Continuity Planning
  - Security Consulting
  - Bewußtseinsbildung
  - Schulung / Ausbildung
  - Produktevaluation

Schlüssel zum Erfolg

- Notwendig:
  - Klares Verständnis
  - Klare Zielvorgaben und Rahmenbedingungen
  - Gesicherte Unterstützung und Finanzierung
- Wichtige Vorbedingungen:
  - Policies und Verfahrensbeschreibungen
  - Gepflegte Liste der „richtigen“ Kontakte

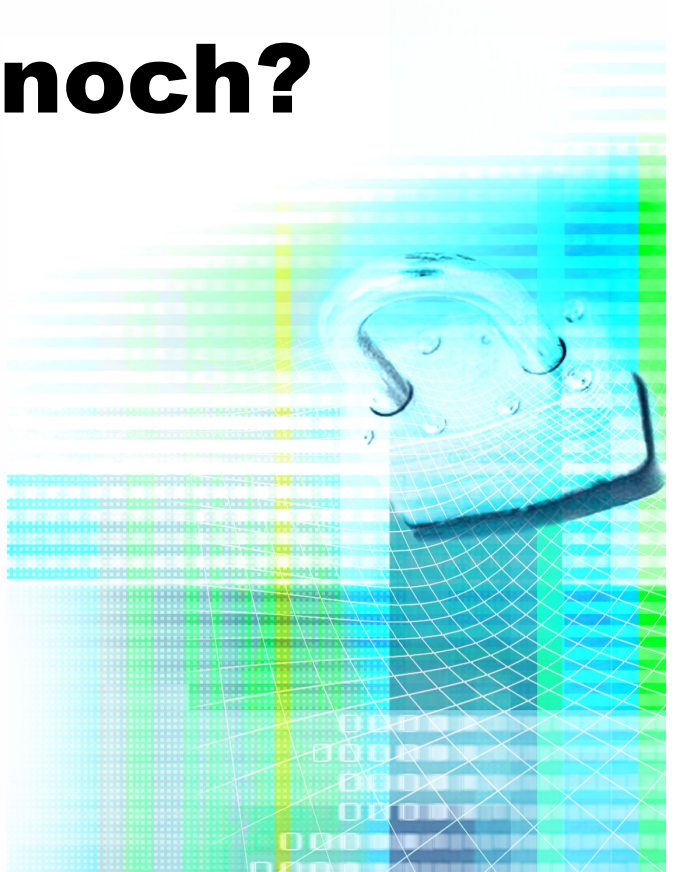
Schlüssel zum Erfolg (2)

- Ohne Kommunikation klappt nichts:
  - Management
  - Benutzer und Administratoren
  - Andere CERTs
- Andere CERTs helfen üblicherweise gerne
  - ... haben aber keine Blaupause für andere Fälle

➲ ***Entscheidung für die richtige Rolle !***

DFN CERT

... und was fehlt noch?



Früh gewarnt, ist halb ...

- IT-Frühwarnung funktioniert auf operativer und taktischer Ebene!
- Frühwarnungen und Informationen benötigen etablierte Arbeitsabläufe, um vor Ort präventive Maßnahmen wirken zu lassen
  - analoges Problem bei den koordinierenden tätig werdenden Notfallteams
  - Verzahnung mit Prozessen unabdingbar
    - des Risikomanagements (vorausschauend)
    - des IT-Sicherheitsmanagements (operativ)
    - des Krisenmanagements (reaktiv)

Open Source Informationen?

- Sicherheitsexperten „leben“ das „Need to Know“ Prinzip
  - Vermiedene Peinlichkeit eigener Lücken
  - Gefühlte Sicherheit durch Totschweigen
- Aber
  - Verlangen nach Informationen anderer !?!

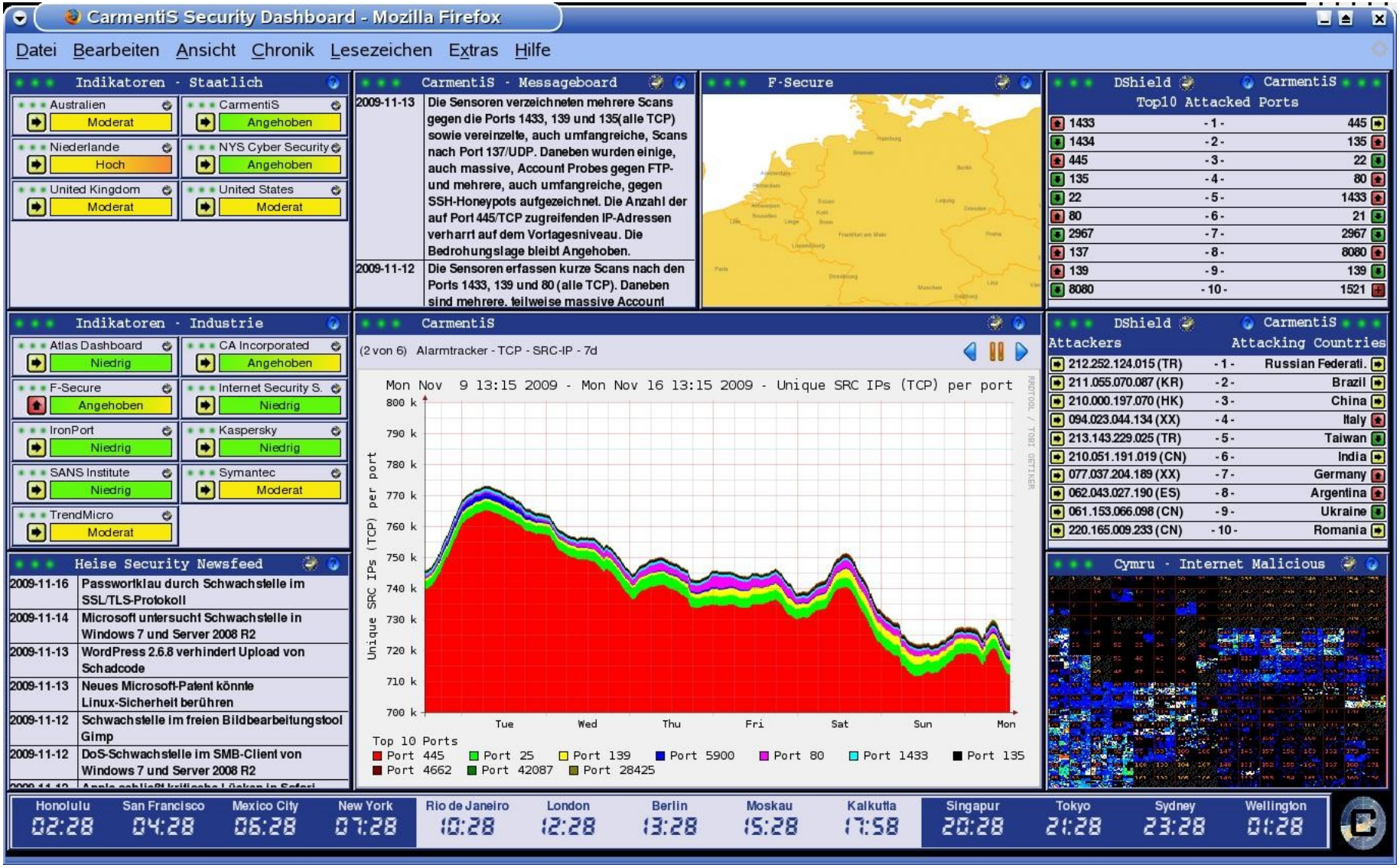
Open Source Informationen!

- Sicherheitsexperten „leben“ das „Need to Know“ Prinzip
  - Verlangen nach Informationen anderer
  - Vermiedene Peinlichkeit eigener Lücken
  - Gefühlte Sicherheit durch Totschweigen
- Nur langsam setzt sich das Bewußtsein durch, dass es ein „Need to Share“ gibt
  - Zumindest wenn es um übergeordnete Interessen geht
  - Geeignete Werkzeuge fehlen jedoch

IT-Sicherheitslagebild

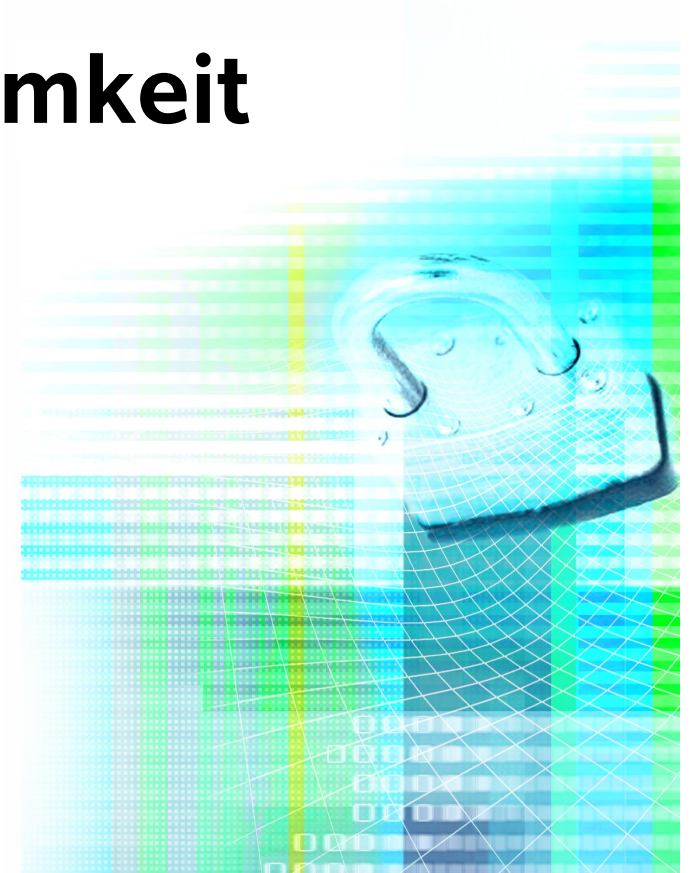
- Notwendiger Teil des operativen IT-Sicherheitsmanagements
- Voraussetzung für ein wirkungsvolles IT-Krisenmanagement
- Genaue Ausprägung weitgehend ungeklärt
  - Konventionelle Listen von Meldungen
  - Zunehmend Dashboard-Ansätze
- Bedarf auf unterschiedlichen Ebenen
  - Need-to-Know Prinzip überwiegt weiterhin und verhindert übergeordnete Lagebilder

Security Dashboard



DFN CERT

Vielen Dank
für Ihre Aufmerksamkeit



Dr. Klaus-Peter Kossakowski
klaus-peter@kossakowski.de

Kontakt

Dr. Klaus-Peter Kossakowski

Email: klaus-peter@kossakowski.de
Mobil: (+49) 0171 / 5767010