



Session 1: Wirtschafts-CERT und deren Ausbau zu einem IT-Frühwarnsystem

Martin Voitke
martin.woitke@secunet.com

BITKOM IT-Frühwarnsysteme 2004

- Mitglied im BITKOM AK „IT-Frühwarnsysteme“
- Mitglied in der CERT AG
- Mitglied im FIRST (Forum of Incident Response and Security Teams)
- betreibt das interne secuCERT seit 1999
- ist ein deutscher IT-Sicherheitsdienstleister
 - Analyse
 - Beratung
 - Realisierung
 - Lösungen
 - Support
- betreut und unterstützt Kunden aus Wirtschaft und Verwaltung



- 13:15 Start Session 1
- 13:20 Motivation der Entstehung von Warnsystemen bei Computer Emergency Response Teams
- 13:40 Mcert als CERT für die mittelständische Wirtschaft
- 14:00 Kleine Pause
- 14:15 Start der Diskussion
- 15:00 Zusammenfassung der Diskussionsergebnisse
- 15:15 Ende Session 1

„Ein IT-Frühwarnsystem ist eine langfristige verankerte Beobachtung und Analyse IuK-basierter Infrastrukturen mit dem Ziel, Risiken, Schwachstellen und drohende Fehlentwicklungen frühzeitig zu identifizieren, vorbeugende auszuräumen und zu minimieren.“

In Session 3 geht es um das „**frühzeitige Identifizieren von Schwachstellen und Risiken**“.

In Session 2 geht es um interdisziplinäre Methodiken zur Bewertung von „**Risiken und drohenden Fehlentwicklungen**“.

In Session 1 geht es um das „**vorbeugende Ausräumen und Minimieren**“.



Motivation der Entstehung von Warnsystemen bei Computer Emergency Response Teams

BITKOM IT-Frühwarnsysteme 2004
Session 1

>> Ist die Wirtschaft der neuen Bedrohungssituation gewachsen ?

- Bedrohung der IT-Systeme über
 - Würmer
 - Trojaner
 - Denial of Service-Attacks
 - Viren
 - Hacking
 - Terroristische Angriffe auf IT
 - Cyber-War
- **Schnelle Reaktion erforderlich, falls sensible, lebenswichtige Systeme der Wirtschaft betroffen.**
- **Die Vorwarnzeiten für Angriffe aus dem Internet werden immer kürzer.**

- Die finanziellen Gesamtverluste (Schäden durch Angriffe auf IT-Sicherheit) der befragten 530 Unternehmen betrug \$201.797.340 (im Vorjahr \$455.848.000).
- Die Anzahl aller Sicherheitsvorfälle war in etwa identisch mit der Anzahl vom Vorjahr. An erster Stelle lag der Diebstahl von internen Informationen.
- Im Gegensatz zum Vorjahr war lagen Schäden durch Denial of Service-Angriffe an zweiter Stelle mit \$65.643.300, das bedeutet eine Steigerung von 250 %.

Quelle: <http://gocsi.com>

- Schaden bei einem Internet-Provider in Höhe vom 4,5 Millionen Euro
- Angewandte Techniken
 - Fake-Accounts (Betrug durch Angabe falscher Personalien)
 - Missbräuchliche Nutzung echter Kundenzugänge
 - auf Web-Seiten veröffentlichte Zugangsdaten und
 - Ausspähen von Daten mit so genannten „Trojanern“
- 3.600 Tatverdächtige, 79% der Täter waren unter 22 Jahre alt
- 6% der Tatverdächtigen haben selbst „Trojaner“ eingesetzt
- in der Regel „wirtschaftliche Motive“

Quelle: Bundeskriminalamt, www.bka.de, Kriminalistisches Institut – KI 13

- Verbreitung über DCOM RPC-Schwachstelle (Port135) Windows 2000/XP
 - Überlaufschwachstelle (Buffer Overflow) ermöglicht überschreiben von Code-Variablen
 - Command-Interpreter (cmd.exe) wird an Port 4444 gebunden
 - Übertragung des Wurm Msblast.exe über tftp
 - Start des Programms Msblast.exe
 - Erzeugung eines Eintrags in der Registry für Autostart nach Reboot
- Suchen nach weiteren Opfern in einem Klasse-C IP-Netz
- Falls Datum > 15.08 DoS-Angriff auf www.windowsupdate.com

Quelle (u.a.): www.securityfokus.com

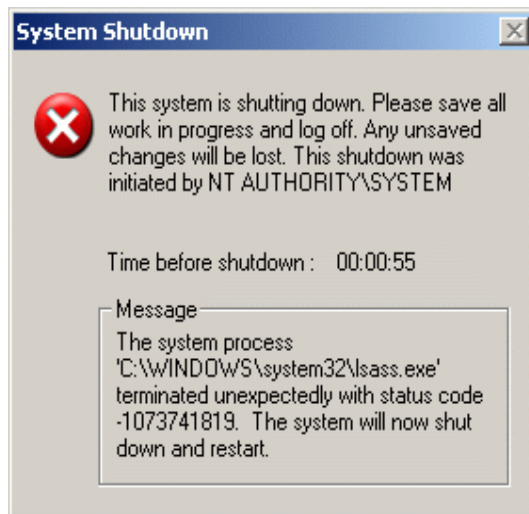
- Frühjahr 2003 DCOM RPC-Schwachstelle bei Windows 2000/XP 2003 war im Prinzip bekannt
- 16.07.2003 Microsoft Security Bulletin und Patch verfügbar
- 10.-18.08.2003 Ausbruch des Wurms, bei ca. 400.000 – 1.4 Mio Computer infiziert, die nicht gepatched waren unterschiedliche Varianten im Umlauf, Virens Scanner konnten auf neue Varianten nicht reagieren, RPC-Sperrung als Firewall-Adhoc-Maßnahme war wirksam.
- 15.08.2003 DoS-Angriff auf windowsupdate.com hatte keinen Schaden angerichtet, da der Dienst herunter gefahren wurde.

- 6,7 % Arbeitsplatz-PC
- 25,5 % Heim-PC
- 4 % Arbeitsplatz-PC und Heim-PC
- 61,2 % Nein
- 2,6 % weiß nicht

6210 Befragte in Deutschland, Start 13.08.2003

Schaden in Millionenhöhe für die Wirtschaft vermutet

Quelle: www.ZDNet.de



- 13.April 2004: Microsoft stellt Security Bulletin und Patch bereit
- 02.Mai 2004: mehrere Varianten von Sasser (A,B,C,D) im Umlauf
- 05.Mai 2004: Sasser (A-D) Worm Removal Tool wurde 1,5 Millionen Mal heruntergeladen
- Angriffe über Schwachstelle beim Local Security Authority Subsystem Service (LSASS), DCOM-Schwachstelle
- Ein FTP Script/Server wird geladen, der den Wurm über FTP nachlädt. Daneben installiert der Wurm eine Hintertür.
- Erzeugt Shutdown-Meldung und installiert sich dauerhaft auf dem Rechnern, scannt nach weiteren Rechnern, die diese Sicherheitslücke aufweisen.

- **Unternehmen verfügen über**
 - Virens Scanner
 - Firewalls
 - IT-Risikomanagement
 - IT-Sicherheitsmanagement
 - IT-Notfallmanagement
 - Z.T. ein internes CERT (Computer Emergency Response Team)

- **haben Informationsschnittstellen zu**
 - externen CERTs
 - IT-Service-Dienstleistern
 - Internet-Informationsquellen



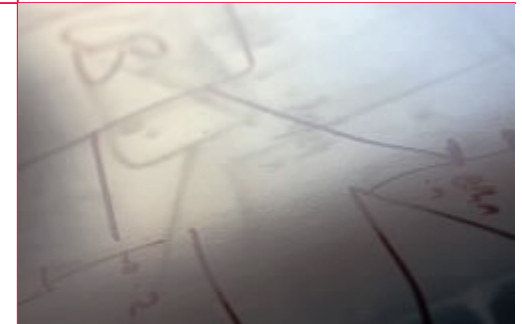
- **Traditionelle CERTs**
 - Softwarehersteller
 - Forschungsnetze
 - Militär
 - Netzbetreiber
 - Länder
- **Neue CERTs für Organisationen sind entstanden**
 - Banken
 - Telekommunikation
 - Automobilindustrie
 - Elektroindustrie
 - Mittelstand (Mcert)
 - Behörden (z.B. BSI CERT-Bund, CERT-Bayern)

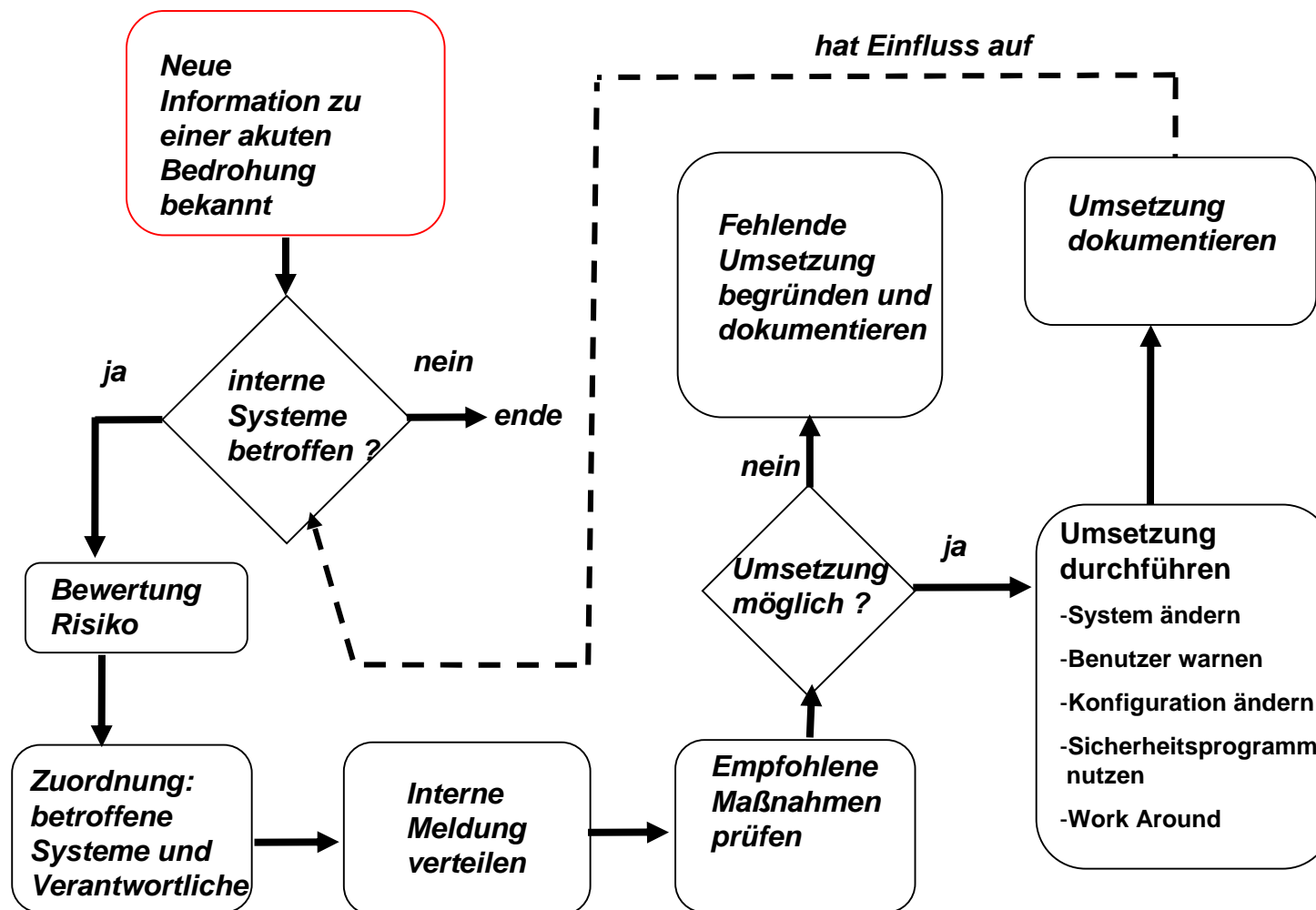


- Gefahrensituation beobachten
- Informationen bewerten
- Bewältigung akut auftauchender Sicherheitsprobleme
- Informationen verteilen und steuern
- Ursachen erforschen
- Zusammenarbeit mit
 - Softwareherstellern
 - IT-Betrieb
 - IT-Management
 - IT-Sicherheitsmanagement
 - Notfallmanagement
 - Krisenstab
 - Netzwerkbetreiber
 - anderen CERTs



- **Erfassung und Bewertung von Meldungen/Alarme**
 - Sind wir überhaupt betroffen?
 - Ist das eine Fehlmeldung (Hoax)?
- **Interne Risikoeinschätzung**
 - Wie groß ist die konkrete Verwundbarkeit?
 - Wie schnell muss eine Lösung erfolgen?
 - Vertraulichkeit der Risikosituation?
- **Genauigkeit und Geschwindigkeit der Reaktion**
 - Was ist die richtige Reaktion?
 - Wer kann entscheiden, was die richtige Reaktion ist?
 - Abhängigkeiten zu anderen Aktivitäten/Systemen?
 - Verfolgung der Umsetzung von Maßnahmen?
- **Notfallplanung für Eskalation**

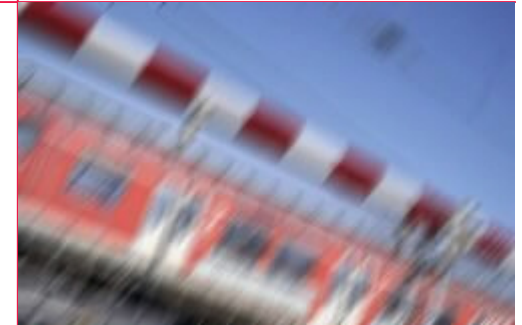




- Informationsmanagement
- Geschwindigkeit
- Genauigkeit
- Konfigurationsmanagement
- Sicherheit der Information
- Kontrolle
- Priorisierung
- Prozesskosten

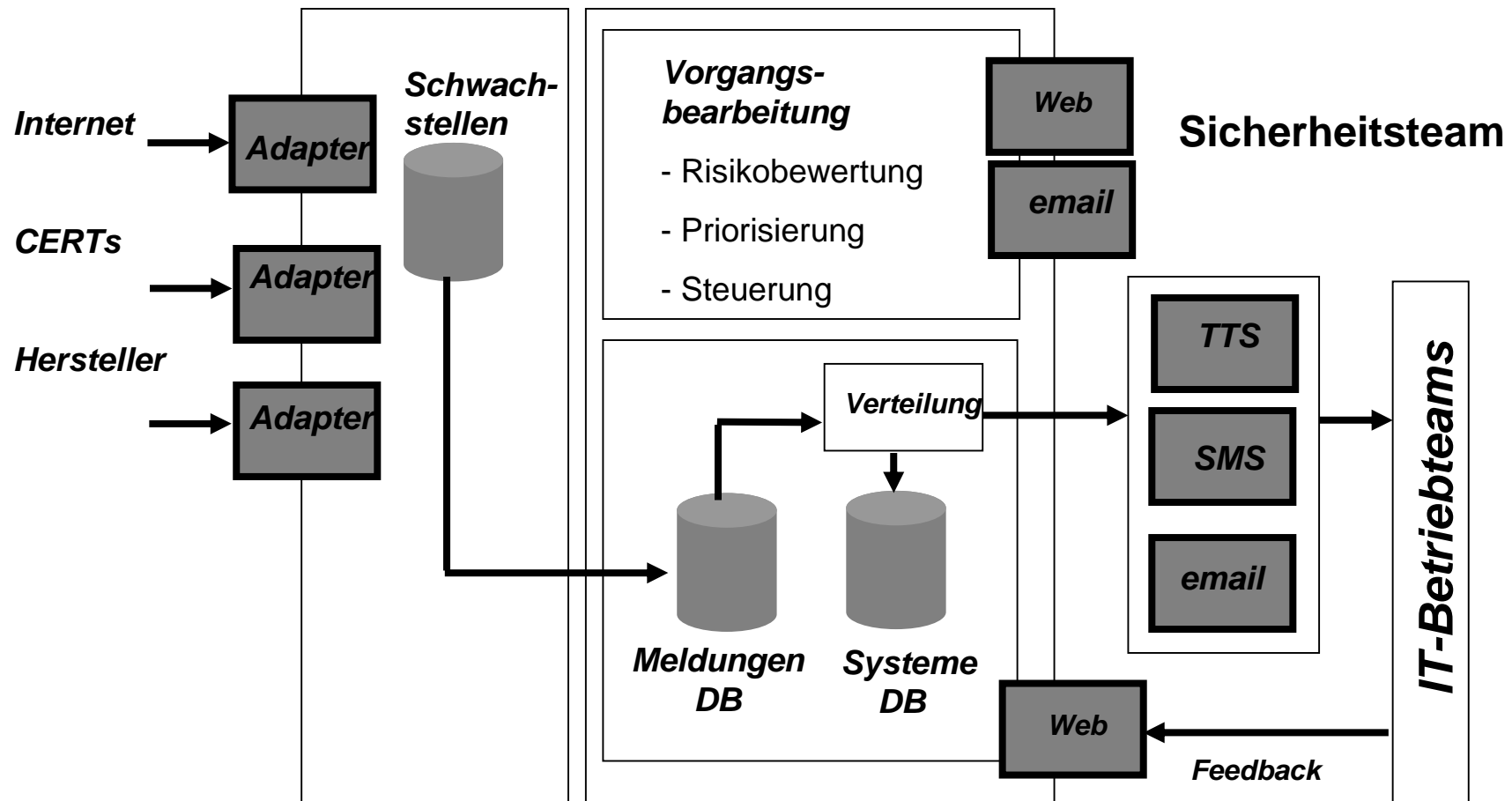


- Schnellere Reaktionen
- Mehr Sicherheit
- Weniger Schäden
- Vermeidung von Fehlalarmen
- Mehr „gesicherte“ Kommunikation
- Mehr Synergien
- Minimierung von Zeit-, Kosten- und Personalaufwänden



- Umsetzung von Prozessen zur individuellen Risiko-Bewertung
- Unternehmensweite Informationsbasis für das Risiko-Management
 - Systeme
 - Konfigurationen
 - Schwachstellen
 - Stand der Bearbeitung von Maßnahmen
- Krisenmanagement
 - Entscheidungsprozesse
 - Kommunikation über sichere Kommunikationsnetze

>> Eine Vision ?
Bearbeitung von CERT-Meldungen





Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

Martin Voitke
martin.voitke@secunet.com

- 13:15 Start Session 1
- 13:20 Motivation der Entstehung von Warnsystemen bei Computer Emergency Response Teams
- 13:40 Mcert als CERT für die mittelständische Wirtschaft
- 14:00 Kleine Pause
- 14:15 Start der Diskussion
- 15:00 Zusammenfassung der Diskussionsergebnisse
- 15:15 Ende Session 1

Wirtschafts-CERT und deren Ausbau zu einem IT-Frühwarnsystem

- Vorgehen
- Vier allgemeine Fragestellungen
- Spontane, freie Diskussion per Wortmeldung
- Abschließende Zusammenfassung des Stimmungsbildes

Risikoszenario: Real oder übertrieben ?

- Diskussion
 - Bedrohungen der Wirtschaft ?
 - Informationsdefizite ?
 - Wird nicht bereits genug getan ?
 - Nur ein aktueller Trend ?
 - Oder langfristiges Risikoszenario ?

Welche Warnsysteme brauchen wir ? Was sind die Voraussetzungen für den Erfolg ?

- Diskussion
 - für die Zielgruppen Unternehmen, Privatpersonen, Behörden
 - Voraussetzungen
 - Erwartungen
 - Ziele
 - Standards
 - Prozesse

IT-Frühwarnsysteme: Wo liegen Gefahren bei der Umsetzung ?

- Diskussion
 - Vertraulichkeit ?
 - Vertrauenswürdigkeit ?
 - Mehr Schaden als Nutzen ?
 - Verantwortlichkeiten ?
 - Erfahrungen aus anderen Bereichen ?

Was wären erste Schritte ?

- Diskussion
 - Beteiligung der IT-Industrie ?
 - Beteiligung der Wirtschaft ?
 - Beteiligung der öffentlichen Verwaltung ?
 - Einbindung in andere Aktivitäten ?
 - Einbindung der CERTs in Deutschland ?
 - Plan und Vorgehen ?



Vielen Dank für Ihre Mitwirkung

Martin Voitke
martin.voitke@secunet.com