

CERT BWL

Computer **E**mergency **R**esponse **T**eam
Baden-**W**ürttemberg **L**andesverwaltung

IV.1 Aufbau eines virtuellen CERT in der Landesverwaltung Baden-Württemberg

**43. Erfahrungsaustausch des KoopA ADV
6. und 7. März 2006 in Hamburg**

Dr. Rolf Häcker, Gerhard Polifke, Dr. Marcus Schweizer



Baden-Württemberg

Informatikzentrum

Landesverwaltung Baden-Württemberg (IZLBW)

DAS IZLBW stellt sich vor

- **Rechenzentrum der Landesverwaltung BW**
- **Aufgaben**
 - **Landesverwaltungsnetz LVN**
 - **Serverhosting**
 - **Client-Betreuung**
 - **Zentrale Netzdienste**
 - **Zugänge zum Internet, TESTA, KVN**
 - **Anwendungsentwicklung**



Agenda

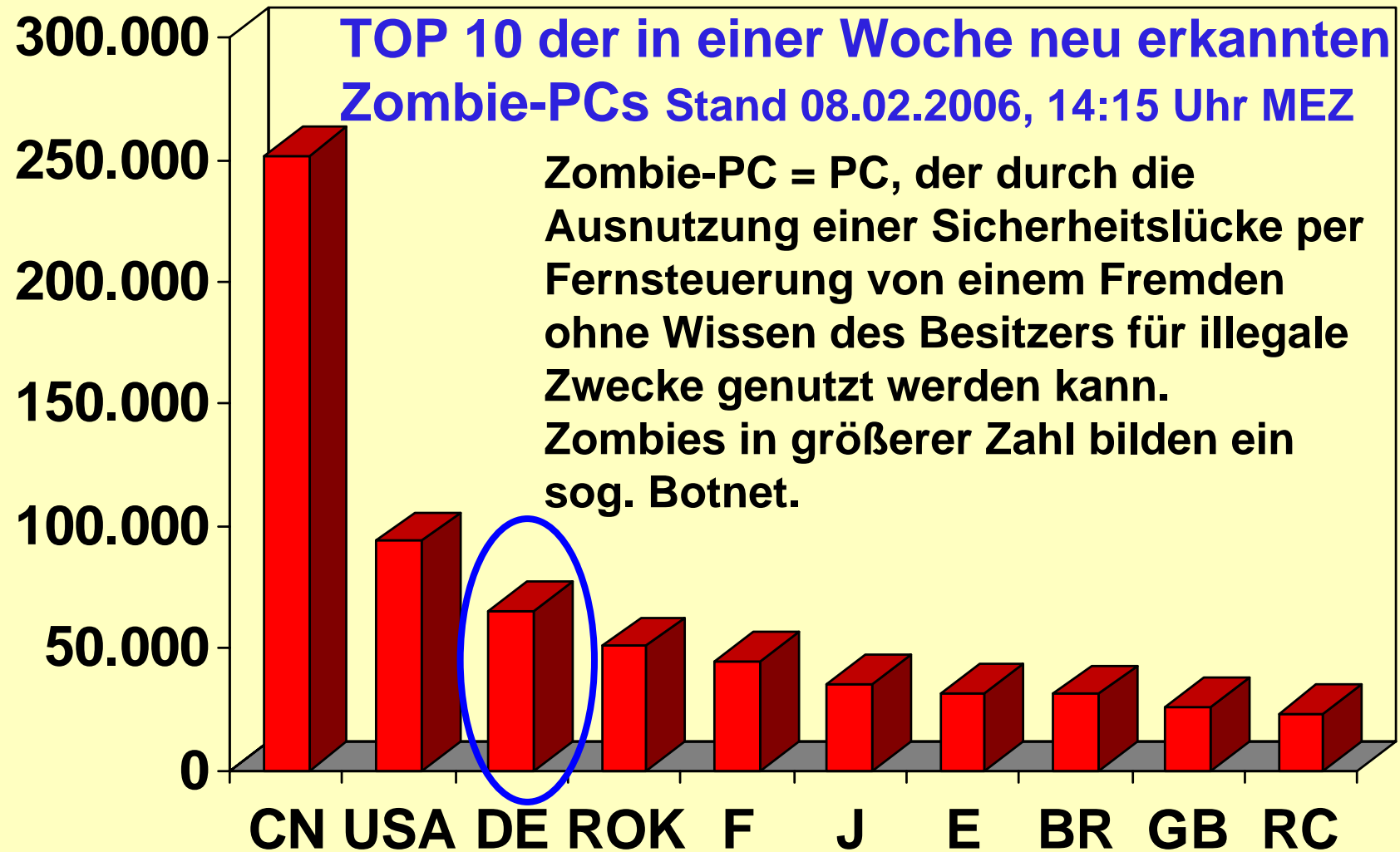
- **Bedrohungslage**
- **Gegenmaßnahmen und Motivation für das CERT BWL**
- **Planung und Umsetzung**
- **Zusammenfassung**





Bedrohungs-lage

Bedrohungslage Zombie-PCs ...

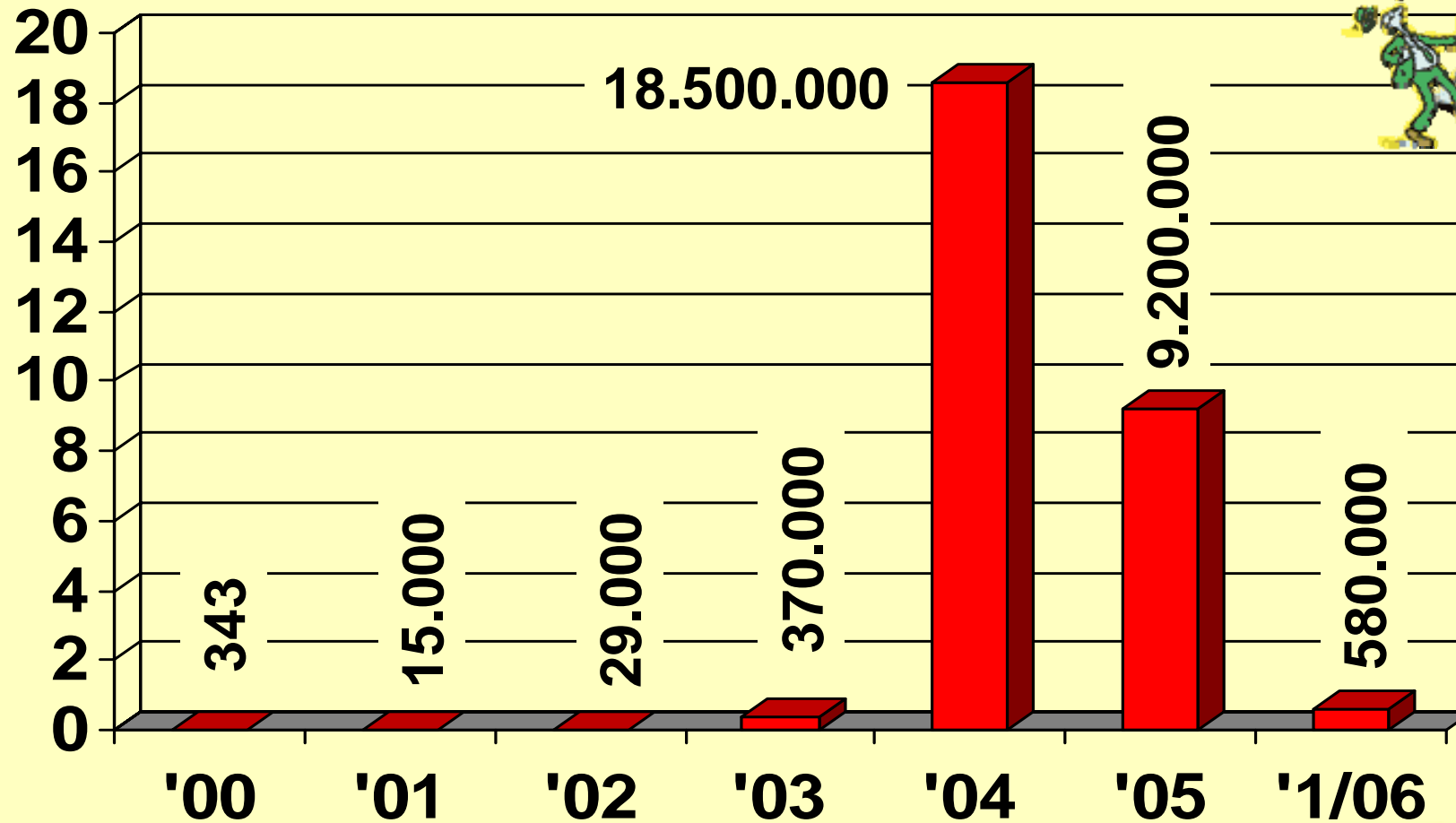
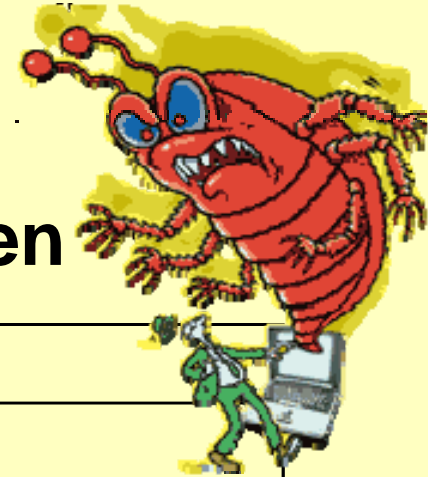


Quelle: CIPHERTrust
(www.ciphertrust.com)



... Viren ...

Durch das IZLBW abgefangene Viren



... Viren und Trojaner im Mailverkehr ...

	Viren (im LVN)	Viren (Internet)	Trojaner (im LVN)	Trojaner (Internet)
07/2000		343		
2001		15.000		
2002	345	29.000		
2003	1.400	370.000	50	4
2004	96.000 23 Mio. Mails	18.500.000 42 Mio. Mails	8.800	13
2005	20.000 43 Mio. Mails	9.200.000 49 Mio. Mails	28.000	311






... und andere Gefahren

- manipulierte Bilder oder Musikstücke installieren
Spionage- und Fernsteuer-Programme auf dem PC
- immer raffiniertere und aggressivere Werkzeuge
forschen Bankdaten oder Firmengeheimnisse aus
- mit großflächigen Angriffen mittels Zombie-PCs
werden Unternehmen erpresst (DDoS)
- bösartige Programmteile in Spielen oder Klingeltönen
machen Handys unbrauchbar
- **durchschnittlich 16 neue Sicherheitslücken in
Systemen und Anwendungen werden täglich
gemeldet**



Gegenmaßnahmen und Motivation für das CERT BWL

Sofortmaßnahmen bei einem Sicherheitsvorfall:

-  Schadensbegrenzung (z.B. Trennung befallener Systeme vom Netz) und Ursachenforschung
-  Warnung und Information weiterer Gefährdeter
-  Sicherung von Beweismaterial
-  Behebung des Schadens
-  Schließen der Sicherheitslücke



Vorsorge zur Vermeidung von Sicherheitsvorfällen

Damit es erst gar nicht so weit kommt:



- frühzeitige breit gestreute Informationen über erkannte Sicherheitslücken und Abwehrmaßnahmen
- Einsatz von stets aktuellen Abwehrprogrammen gegen Viren und andere Angriffe
- Schließen bekannter Sicherheitslücken (z.B. durch Installation von Programmkorrekturen der Hersteller)
- regelmäßige Datensicherung und Übung der Datenwiederherstellung

Vieles wird schon getan, aber ...

- mehrere IuK-Dienstleister im Land erledigen vergleichbare Sicherheitsaufgaben (z.B. in Steuer-, Umwelt- und Innenverwaltung)
- durch mehrfache ganzheitliche Bearbeitung entsteht so Parallel- und Doppelarbeit
- gleiche Informationsquellen werden teilweise mehrfach ausgewertet
- bisher kaum Informationsaustausch zwischen den IuK-Dienstleistern im Land

Vorteile eines CERT BWL

- Aufgabenbündelung an einer Stelle, wo immer es zweckmäßig ist
- Einbindung von Sicherheitsaufgaben und Expertenwissen vor Ort in ein Gesamtkonzept (virtuelles CERT)
- Intensivierung und Koordination des Informationsaustausches untereinander
- Intensivierung und Koordination der Zusammenarbeit mit anderen CERTs.

Dienstleistungen des CERT BWL

➤ Prävention

- Verteilung von Sicherheitsinformationen
- Informations- und Erfahrungsaustausch

➤ Reaktion

- Prüfung und Bewertung von Meldungen zu Sicherheitsvorfällen
- Warnung, Unterstützung und Beratung
- Koordination von Abwehrmaßnahmen

➤ Sicherheits-Qualitätsmanagement

- Bewusstseinsbildung

Aufbau und Planung des CERT BWL (1)

- Einrichtung eines Projektkernteams
- Definition der CERT-Aufgaben im Team
- Konzeption der Aufgabenverteilung im Team
- Vereinbarung von Diensten, Dienstgüte, Pflichten und Kompetenzen der CERT BWL-Teilnehmer

Aufbau und Planung des CERT BWL (2)

- Aufbau bzw. Ausbau der CERT-Fachkompetenz
- Auf- und Ausbau von Kontakten mit nationalen und internationalen CERTs
- Aufnahme des CERT BWL in die e-Government-Standards





Planung und Umsetzung

Planung auf vorhandener Struktur

Grundlage: Virenschutzkonzeption der Landesverwaltung

- **Zentrale Virenschutzkomponenten**
 - Mail-Gateways innerhalb des LVN und zum Internet
 - HTTP-Proxys zum Internet mit Virenschutz
 - Zentrale Virensignatur-Verteilserver
 - Virenschutz auf Netzdienste-Servern
- **Lokale Virenschutzkomponenten**
 - Virenschutz auf Clients und Servern in Dienststellen
 - Lokale Virensignatur-Verteilserver
- **Benachrichtigung der Benutzer**
 - Vireninformationen & -meldungen
- **Beratung & Unterstützung bei Virenvorfällen**

Sicherheitsvorfälle und Anfragen

- **Einbindung des Sicherheitsteams des IZLBW**
 - Beratung zu Sicherheitsfragen (z.B. Verschlüsselung, VOIP, Wireless LAN, VPN-Technik)
 - Bearbeitung von Sicherheitsvorfällen (teilweise für Kunden des IZLBW)
 - Erstellung von Stellungnahmen und Sicherheitskonzepten

- **Einbindung der Sicherheitsteams der beteiligten IuK-Zentren**

Verteilung von Informationen

- Annahme, Bewertung und Behandlung von Sicherheitsvorfällen der Kunden
- Annahme und Bewertung von Sicherheitsinformationen anderer CERTs oder von anderen Quellen
- Gezielte Informationsweitergabe an die Mitarbeiter und Kunden
- Vertrauliche Behandlung von Sicherheitsvorfällen

Verteilung von Patches

- Durch Patchmanagement-Teams
- Sammlung, Bewertung & Weiterleitung von Patches der Hersteller (z.B. von Microsoft, HP)
- Team besteht aus Mitarbeitern von verschiedenen Dienststellen der Landesverwaltung

Infrastruktur

- **Abwicklung und Dokumentation der Anfragen und Sicherheitsvorfälle**
 - Einsatz eines Ticket-Systems, z.B. Service-Desk
- **Sicherstellung der Vertraulichkeit**
 - Ggf. disziplinarische, zivilrechtliche oder gar strafrechtliche Konsequenzen)
- **abgesicherte Umgebung**
 - Netz, Dateiablagestruktur, Drucker, sicheres CERT-Team-Postfach

Organisation des virtuellen CERT (1)

➤ **CERT-Manager**

- Koordination der Aufgaben des CERT BWL
- Einbindung und Steuerung der Mitarbeiter in den (verteilten) Dienststellen

➤ **CERT-Büro**

- Unterstützung des CERT-Managers
- Abwicklung von (Routine)-Aufgaben
- Anlaufstelle des CERT BWL

Organisation des virtuellen CERT (2)

➤ CERT-Team

- Mitarbeiter aus den beteiligten Dienststellen
- Analyse, Bewertung und Aufarbeitung von Sicherheitsvorfällen
- Handlungsempfehlungen bzw. Vorgaben!
- Vorbeugende Maßnahmen:
Informationen, Empfehlungen,
Handreichungen

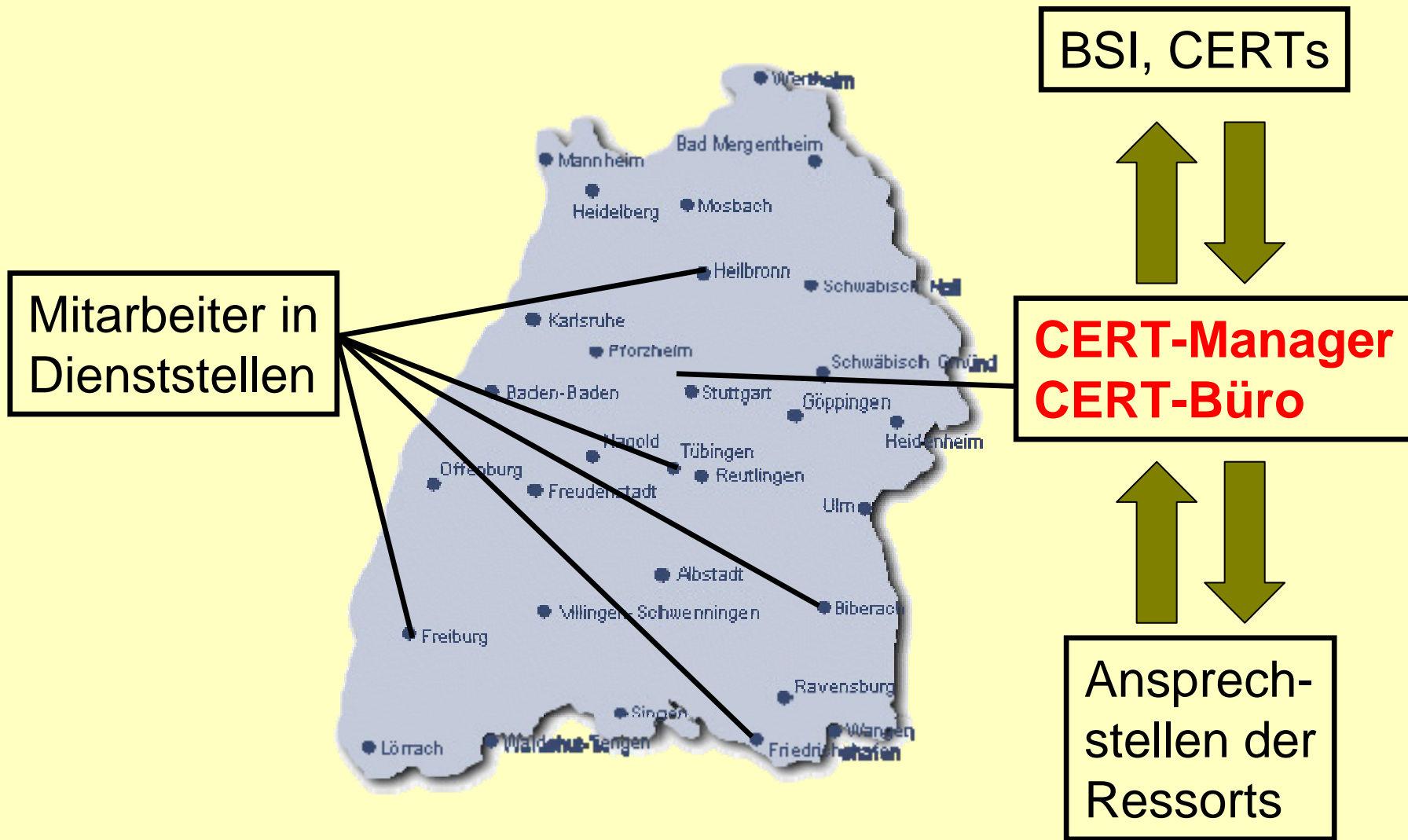
Mögliche Schwächen eines virtuellen CERT

- **Kein zusätzliches Personal;**
Aufgaben sollen durch bestehendes Personal erledigt werden
- CERT-Teammitglieder sind durch ihre Regeltätigkeit gebunden
- Priorisierungskonflikte mit Regelaufgaben
- Evt. aufwändigere Abstimmung und Kommunikation

Voraussetzungen für das Gelingen

- Zentrale Kommunikation
- Rückhalt in der Führungsebene
- Geeignete Gestaltung des CERT-Teams
- Regelmäßige Treffen und intensive Kommunikation

Zusammenarbeit im CERT-BWL

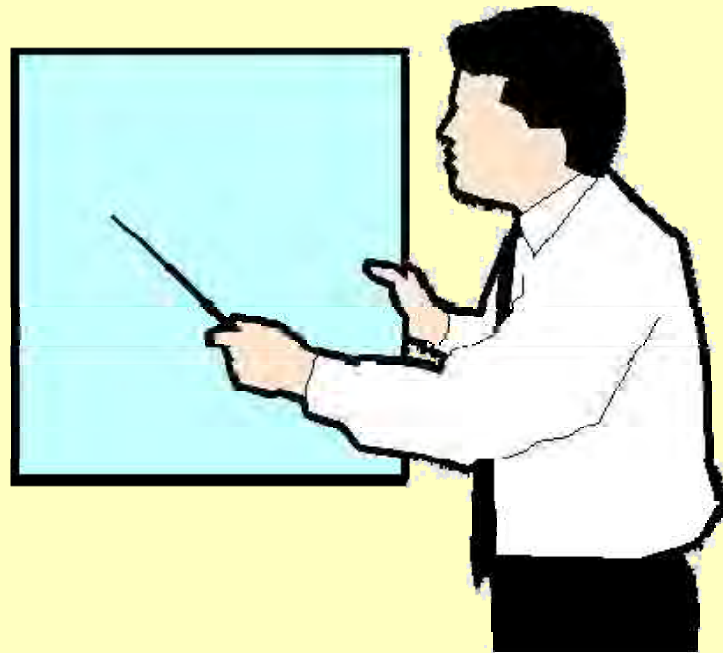


Projektverlauf CERT BWL

- **Juli 2005:** Startveranstaltung
- **Ab August 2005:**
 - Aufgabenbeschreibung und Besetzung des Projektkernteam
 - Teilnehmer aus beteiligten IuK-Zentren
 - Vorbereitung und Planung
 - Formulierung des Projektauftrags
 - Festlegung und Verteilung der Aufgaben
- **Februar 2006:**
 - Projektauftrag an das IZLBW

Vorgesehene weitere Planung

- Erstellung des Feinkonzepts bis Ende Juni 2006
- Start des CERT BWL ab Juli 2006

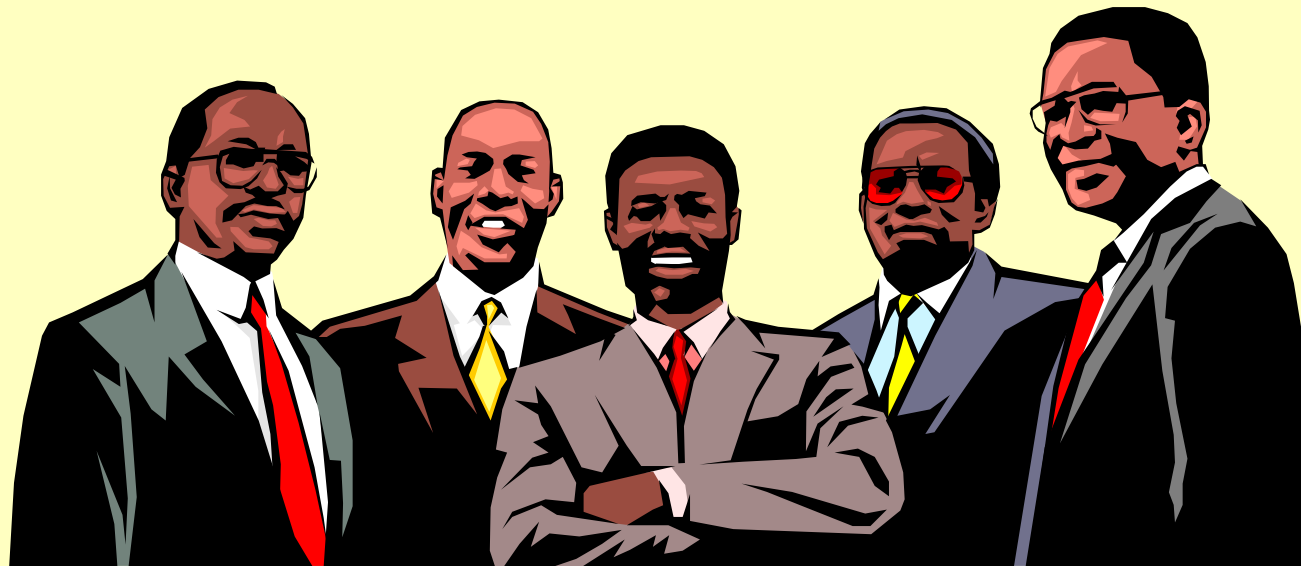


Was bisher erreicht wurde

- ☑ Mitgliedschaft in CERT-Verbund und CERT-AG
- ☑ Projektauftrag und Organisationsmodell vom BSI geprüft und positiv kommentiert
- ☑ Projektauftrag wurde innerhalb der Landesverwaltung abgestimmt und dem IZLBW erteilt
- ☑ Projektkernteam wurde eingerichtet
- ☑ Informationsaustausch zwischen beteiligten Sicherheitsteams und Sicherheitsbeauftragten

Was noch zu tun ist

- Einigung über Definition der Aufgaben und Konzeption der Aufgabenverteilung („Feinkonzept“)
- Abschluss von Vereinbarungen zu Diensten, Dienstgüte, Pflichten und Kompetenzen
- Einrichtung der Kopfstelle im IZLBW und Auf- bzw. Ausbau des CERT-Teams in Stufen
- Einbindung des CERT-Teams in die CERT-AG
- Ergänzung der E-Government-Standards um Regelungen zum CERT BWL als Dienstleister der Landesverwaltung

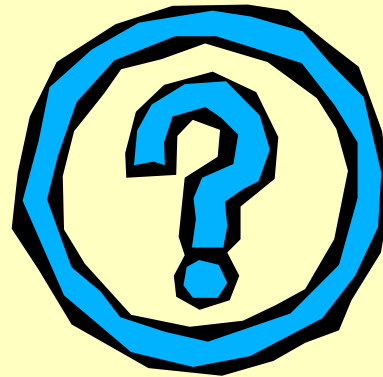


Zusammenfassung

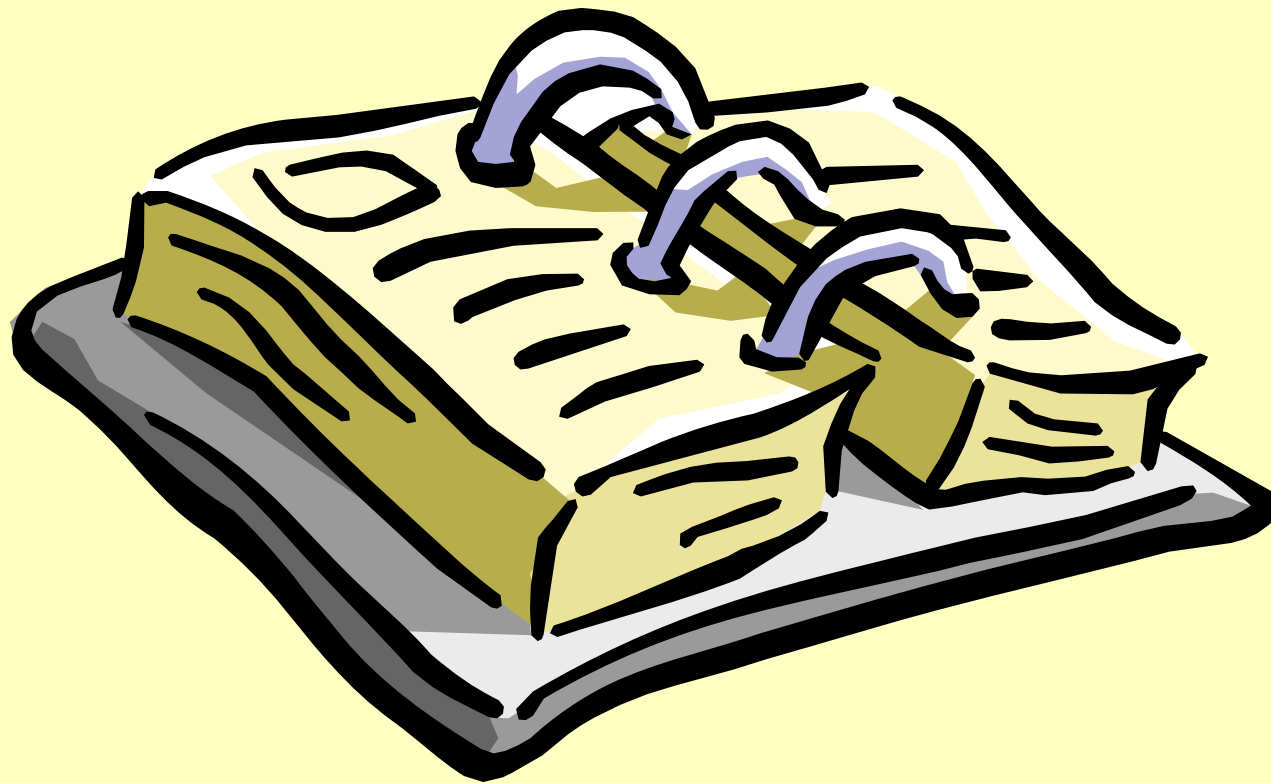
Zusammenfassung

- Reale vielschichtige Bedrohungslage zwingt zum Handeln
- **Lösung: Einrichtung eines CERT**
- Problem: keine zusätzlichen Personalressourcen
- Plus: Erfahrungen im Umgang mit Sicherheitsproblemen vorhanden
- **Einrichtung eines virtuellen CERT BWL** zur Bündelung der verteilten Kräfte unter zentraler Steuerung
- **Umsetzung wurde bereits begonnen**

**Vielen Dank für Ihre
Aufmerksamkeit!**



Ihre Fragen ?



Anhang

Unterstützung für das CERT BWL



**Bundesamt für Sicherheit in der
Informationstechnik (BSI)**

Mentor für den Aufbau des CERT BWL



CERT-AG

Arbeitsgemeinschaft von ca. 30 deutschen CERT
StaV des Innenministeriums ist Repräsentant für das
CERT BWL



CERT-Verbund

Allianz deutscher Sicherheits- und Computer-
Notfallteams aus Verwaltung, Wirtschaft und Industrie

Unterstützung durch das BSI



Warn- und Informationsdienste-Portal

kundenspezifische Informationsangebote orientiert an Technik, Risikostufen und zeitlicher Erreichbarkeit



CERT-Bund Alarmierungssystem

kann in kritischen Situationen rund um die Uhr automatisiert Administratoren und Entscheidungsebenen alarmieren



Frühwarnsystem

Auswertung von Aktivitäten im Internet soll zu Früh- bzw. Vorwarn-Systemen führen



Vorfallbearbeitungssystem für CERTs

Software zur Bearbeitung von Vorfällen im Verbund der CERTs, Basis für eine gemeinsame Dokumentation und Statistik

Zusammenarbeit im CERT BWL

