

Cyber Defence – Schutzlos in einer vernetzten Welt?

Das CERT Bundeswehr

Bonn
16.02.2009



Bundesamt für Informationsmanagement
und Informationstechnik der Bundeswehr

Oberstleutnant

Norbert Wildstacke

InfoOp / CNO / CIIP

IT-AmtBw A6
Alte Heerstraße 149
D-56076 Koblenz

Tel.: +49 261/896-83 56
Fax: +49 261/896-83 65

E-Mail: NorbertWildstacke@Bundeswehr.org



Copyright 2002 by Randy Glasbergen.
www.glasbergen.com



“I’m sorry, but we don’t allow laptop computers on board. The cursor can be used as a weapon.”

Wer bedroht uns eigentlich?



Terroristen



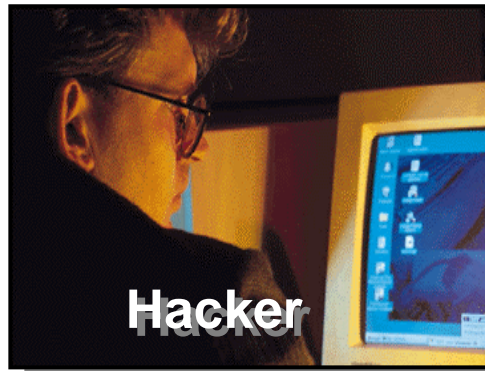
**Traditionelle
Geheimdienste**
(Freund & Feind)



**Andere
Nachrichten-
dienste**



Insider



Hacker



**Kriminelle
Elemente**

“Durch den Gebrauch öffentlich zugänglicher, nicht richtig geschützter Quellen ist es möglich, insgesamt rund 80% der benötigten Informationen über den Feind zu beschaffen!”

Al-Qaeda Trainingshandbuch



Make love, not war!

www.bundeswehr.de

Original ...

Bundeswehr

Kontakt Sitemap Suche >OK Ministerium Presse

WIR ÜBER UNS STREITKRÄFTE VERWALTUNG REFORM KARRIERE JUGEND SERVICE

Einsatz im Ausland

Alle Hintergründe zu ISAF, KFOR, SFOR etc. > weiter

Der Minister, das Ressort, Presse, Sicherheitspolitik > weiter

99+02 Luna-Aufklärungsdrohne: Deutschland unterstützt UN-Inspektoren im Irak > weiter

ABC-Kräfte in Kuwait - Generalinspekteur erwägt Verstärkung "zum Selbstschutz der Soldaten" > weiter

Reportage: So wird das deutsche ISAF-Kontingent versorgt > weiter

Schnelle Verfügbarkeit: Übung "Rapid Guardian" bekräftigt neues Operatives Konzept > weiter

owned by Dr. Gonzo & Raoul Duke - Mozilla {Build ID: 2002121215}

File Edit View Go Bookmarks Tools Window Help Debug QA

http://www.bundeswehr.de/

Home Bookmarks The Mozilla Or... Latest Builds Members-Stat... distributed.ne... linuxforen.de... linuxforen.de... PHPDeveloper... Schulzentrum...

WinFuture.de - Das online Magazin owned by Dr. Gonzo & Raoul Duke

make love, not war ;)

greetings fly out to:
littleSmoke, SunSun23 & r3d33m3r
and especially to the great Blues Brothers

that you're not paranoid doesn't mean they aren't right behind you!

regards,
Dr. Gonzo & Raoul Duke

... und Fälschung

Sonntag, 19.01.2003 ca. 13:10 – 14:50 Uhr

Estland 2007

- Massive DDoS Angriffe auf öffentliche Webseiten (Regierung, Banken, Zeitungen)



[Home](#) [Newsticker](#) [7-Tage-News](#) [News-Archiv](#) [Leserforum](#)

[heise online](#) > [News](#) > [2007](#) > [KW 22](#) > "In Estland wurde der Cyber-Krieg getestet"

29.05.2007 18:41



"In Estland wurde der Cyber-Krieg getestet" vorlesen

Der estnische Ministerpräsident Andrus Ansip hat gegenüber dem [Berliner Tagesspiegel](#) Vorwürfe erneuert, wonach Russland für die [wochenlange Blockade](#) von Webseiten der Regierungsbehörden in Estland verantwortlich sei. "In Estland wurde das Modell eines neuen Cyber-Krieges getestet", sagte Ansip dem [Tagesspiegel](#) (Mittwochs-Ausgabe). Zum ersten Mal überhaupt sei ein unabhängiger Staat solchen Internet-Angriffen ausgesetzt gewesen. Estland ist eines der [am stärksten auf das Internet setzenden Länder](#) der EU und [Vorreiter beim E-Government](#).





Sie sind Gast

[Einloggen](#) | [Registrieren](#)

Suche

News

[7-Tage-Alerts](#)

[7-Tage-News](#)

[News-Archiv](#)

[Newsletter](#)

[English News](#)

News

Meldung vom 30.11.2007 08:25

[<< Vorige](#) [\[Nächste\]](#)

Neuseeländer soll Botnetz mit 1,3 Millionen Computern gesteuert haben vorlesen

Ein 18-Jähriger wird in Neuseeland verdächtigt, mehr als 1,3 Millionen Computer weltweit mit einem Wurm infiziert und damit ein Botnetz aufgetrieben zu haben, über das die infizierten Computer ohne Wissen deren Anwender anderem zu DDoS-Angriffen benutzt wurden. Unter anderem soll das Botnetz für einen Angriff auf IRC-Server und Systeme von Sicherheitsfirmen eingesetzt worden sein, bei dem versehentlich auch ein Server der Universität von Philadelphia lahmgelegt wurde, berichten australische und neuseeländische Medien.

- Georgien 2008

Schlagzeilen | TV-Programm | RSS | Newsletter |

SPiegel ONLINE NETZWELT

NACHRICHTEN | VIDEO | ENGLISH | EINESTAGES | FORUM | SPIEGEL WISSEN

Home | Politik | Wirtschaft | Panorama | Sport | Kultur | **NetzWelt** | Wissenschaft

Nachrichten > NetzWelt > Web > Konflikt im Kaukasus



KONFLIKT
im
KAUKASUS

[Alle Artikel](#)

11.08.2008 [Drucken](#) | [Senden](#) | [Bookmark](#) | [Leserbrief](#) | [Merken](#)

CYBER-KRIEG Schrift:

Hacker fegen georgische Regierungsseiten aus dem Netz

Von Frank Patalong und Christian Stöcker

Seit dem Wochenende sind nur noch wenige georgische Regierungsseiten online erreichbar. Die dortige Regierung hat ihre offiziellen Seiten auf Google-Blog-Server verlegt. Hinter den Attacken sollen russische Hacker stecken. Auf anderen Webseiten tobt längst ein digitaler Propagandakrieg.

MO

Ne

1

2

3

4

5

VII





Guten Tag, mein Name ist Conficker



News

Meldung vom 21.11.2008 10:56

[<< Vorige] [Nächste >>]

Sie sind Gast

[Einloggen](#) | [Registrieren](#)

Suche

News

7-Tage-Alerts

US-Armee untersagt Nutzung von USB-Sticks vorlesen

Ab sofort dürfen Angehörige der US-Armee keine USB-Sticks, CDs, Flash-Media-Karten, Floppys und andere mobile Datenträger mehr an PCs benutzen, [berichtet](#) das Online-Magazin Wired. Der Befehlshaber des U.S. Strategic Command habe die Nutzung sowohl im internen Secret Internet Protocol Router Network als auch im Non-Secure Internet Protocol Router Network bis auf weiteres untersagt.





News

Meldung vom 27.11.2008 11:13

[<< Vorige] [Nächste >>]

Sie sind Gast
[Einloggen](#) | [Registrieren](#)

Suche

News

[7-Tage-Alerts](#)

[7-Tage-News](#)

[News-Archiv](#)

[Newsletter](#)

Windows-Wurm nimmt an Fahrt auf vorlesen

Microsoft beobachtet derzeit die zunehmende Verbreitung eines neuen Windows-Wurms, der die seit mehreren Wochen [bekannte Lücke](#) in den RPC-Funktionen des Server-Dienstes ausnutzt, um in Systeme einzudringen. Insbesondere in Firmennetzen soll die derzeit beobachtete Variante Conficker.A an Fahrt zunehmen. Die meisten Meldungen liegen nach Angaben des Microsoft Malware Protection Centers aus den USA vor. Aber auch Kunden aus Europa, Asien und Südamerika seien betroffen. Zudem lägen Microsoft Berichte von mehreren hundert Heimanwendern vor.

Anzeige





News

Meldung vom 07.01.2009 16:21

[<< Vorige] [Nächste >>]

Sie sind Gast
[Einloggen](#) | [Registrieren](#)

Suche

News

[7-Tage-Alerts](#)

[7-Tage-News](#)

[News-Archiv](#)

[Newsletter](#)

Microsoft: Kunden spielen "Russisches Roulette" mit ihren Systemen



vorlesen

Microsofts Support für die EMEA-Region hatte zum Jahreswechsel ordentlich zu tun, [berichtet](#) Microsoft-EMEA-Sicherheitschef Roger Halbheer in seinem Blog. Schuld war laut Halbheer der Ausbruch einer neuen Variante des Conficker-Wurms, die eine seit Ende Oktober 2008 bekannte Schwachstelle in den RPC-Funktionen des Server-Dienstes ausnutzt, um in Systeme einzudringen. Obwohl Microsoft einen Patch (MS08-067) außer der Reihe bereits Ende Oktober veröffentlicht hat, haben ihn offenbar zahlreiche Kunden immer noch nicht installiert.

Anzeige



online



Sie sind Gast

[Einloggen](#) | [Registrieren](#)

Suche

los

News

[7-Tage-Alerts](#)[7-Tage-News](#)[News-Archiv](#)[Newsletter](#)

News

Meldung vom 12.01.2009 18:43

[<< Vorige](#) | [Nächste >>](#)

Conficker in Kärnten: Nach der Landesregierung nun die Spitäler vorlesen

Nach den [Computern der Kärntner Landesregierung](#) hat der Conficker-Wurm auch die PCs der Kärntner Krankenanstaltengesellschaft [KABEG](#) in mindestens drei Spitälern befallen. Wie bei der Landesregierung sind auch dort rund 3000 Rechner betroffen. Im Unterschied zur Landesregierung sollen die Krankenhaussysteme allerdings das einschlägige Sicherheitsupdate bereits zuvor installiert gehabt haben. Ein weiterer Unterschied ist, dass es dem Wurm gelungen sein soll, weitere Schädlinge auf die befallenen Spitals-Computer zu laden.



online



News

Meldung vom 14.01.2009 11:37

[\[<< Vorige\]](#) [\[Nächste >>\]](#)

Sie sind Gast

[Einloggen](#) | [Registrieren](#)

Suche

News

[7-Tage-Alerts](#)[7-Tage-News](#)[News-Archiv](#)[Newsletter](#)

Studie: 2,5 Millionen PCs mit Conficker-Wurm infiziert

 vorlesen

Nach Schätzungen des Antivirenherstellers [E-Secure](#) hat der Windows-Wurm Conficker alias Downadup bereits rund 2,5 Millionen PCs infiziert. Da der Wurm die Fähigkeit zum Nachladen von Code habe, sei demnächst wahrscheinlich mit einem größeren Botnetz zu rechnen. Von welchen Domains der Wurm den Code nachlädt, bestimmt er laut F-Secure über einen komplizierten Algorithmus. Dabei generiere er viele verschiedene mögliche Domainnamen, sodass ein Sperren aller kaum möglich sei.

Anzeige

Konf

Die
Aler

GS

Plu

EM

Apj

Typ

Syn

Artik



Sicherheitslücke : Wurm Conficker breitet sich rasant aus - Computer-technik - STERN.DE -

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien

Adresse <http://www.stern.de/computer-technik/computer/:Sicherheitsl%FCcke-Wurm-Conficker/652019>

Rubriken stern.de Suche: Artikel Web

Digital: Computer | Internet | Telefon | Technik | Spiele

Preisvergleich Hardware | Preisvergleich Software | Preisvergleich Spiele & Konsolen

19.01.2009, 16:26 Uhr Diesen Artikel: [Drucken](#) | [Weiterempfehlen](#)

Sicherheitslücke

Wurm Conficker breitet sich rasant aus



© Picture-Alliance

Der Computerwurm Conficker vermehrt sich derzeit übers Netz

Lange Zeit ist es ruhig gewesen um die massenhafte Verbreitung von Computerwürmern, die Rechner befallen und lahmlegen. Doch am Montag sorgte ein Unternehmen mit einer Schätzung für Aufsehen, wonach sich der Wurm Conficker rasant vermehren soll. Demnach soll er sich auf rund neun Millionen Rechnern eingenistet haben.

Conficker kursiert bereits seit November 2008 und nutzt eine Lücke in Windows. Betroffen sind alle Betriebssysteme von Windows. Bekannt sind mittlerweile drei



News

Meldung vom 19.01.2009 12:02

[<< Vorige] [Nächste >>]

Sie sind Gast

[Einloggen](#) | [Registrieren](#)

Suche

News

[7-Tage-Alerts](#)

[7-Tage-News](#)

[News-Archiv](#)

[Newslatter](#)

F-Secure: Jetzt neun Millionen Windows-PCs mit Conficker-Wurm befallen vorlesen

Nach Angaben von F-Secure sollen mittlerweile neun Millionen Windows-PCs mit dem Conficker-Wurm infiziert sein. Da die bislang gemeldeten hohen Zahlen von vielen angezweifelt wurden, hat F-Secure die Methode der Zählung in seinem Blog [veröffentlicht](#). Demnach hat der Antivirenhersteller mehrere der 250 täglich vom Wurm kontaktierten Domains registriert und protokolliert die Verbindungen mit. Dabei zählt F-Secure alle eindeutigen IPs mit.

A

A





Sie sind Gast

[Einloggen](#) | [Registrieren](#)

Suche

News

[7-Tage-Alerts](#)

[7-Tage-News](#)

[News-Archiv](#)

News

Meldung vom 21.01.2009 16:22

Wurm dringt in Systeme der britischen Armee ein vorlesen

Auf zahlreichen Kriegsschiffen der britischen Royal Navy [sorgt](#) einem BBC-Bericht zufolge ein Wurm für Beeinträchtigungen. Ob es sich um den Windows-Wurm [Conficker](#) handelt, ist nicht, allerdings gibt es Hinweise, die seine Beteiligung vermuten lassen. Neben auch Basen der Royal Air Force (RAF) und der Armee vom Wurmbefall betroffen, was zum Ausfall der E-Mail geführt haben soll. Nach Angaben des Verteidigungsministeriums ist der Schädling aber nicht versucht, wichtige militärische oder persönliche Daten anzugreifen, sondern nur der Desinfektion der Systeme.

Associan





News

Meldung vom 22.01.2009 13:16

[<< Vorige] [Nächste >>]

Sie sind Gast

[Einloggen](#) | [Registrieren](#)

Suche

los

News

[7-Tage-Alerts](#)

[7-Tage-News](#)

[News-Archiv](#)

[News-Letter](#)

Microsofts Anleitung zur Deaktivierung der Autorun-Funktion unwirksam vorlesen

Das [US-CERT](#) hat einen "Technical Cyber Security Alert" veröffentlicht, der auf Probleme beim Abschalten der Autorun/AutoPlay-Funktion von Windows hinweist. Offenbar deaktiviert der von Microsoft [beschriebene](#) Weg über das Konfigurieren der Registry-Schlüssel `Autorun` und `NoDriveTypeAutorun` die Autorun- und AutoPlay-Funktionen nicht vollständig. Mit vollständig deaktivierten Funktionen würde weder ein Programm auf einem mobilen Gerät beim Anschluss starten, noch würde der AutoPlay-Dialog mit Vorschlägen für weitere Schritte aufpoppen.



Knowledge Center

- BI & ECM
- Compliance & Recht
- CRM
- Data Center & Server
- ERP
- Green IT
- IT-Services
- IT-Strategie
- Mittelstands-IT
- Mobile & Wireless
- Netzwerke
- Notebook & PC
- Office & Tools
- Open Source
- SCM & RFID
- **Security**
- SOA & BPM

Knowledge Center **Security**

Kampffjets am Boden

Conficker-Wurm legte französische Luftwaffe lahm

09.02.2009 um 16:45 Uhr

Autor(en): pte pte.

Der Computerschädling "Conficker" wütet weiterhin in Netzwerken rund um den Globus.

Mitte Januar legte der Wurm die [Systeme](#) der französischen Luftwaffe lahm. Wie das Webportal [IntellegenceOnline](#) aufgedeckt hat, begann der Virusbefall bereits am 12. Januar. Entdeckt wurde er erst Tage später, als der Schaden bereits so groß war, dass der Flugverkehr schwer beeinträchtigt war, wie aus einem vertraulichen Bericht hervorgeht. Aufgrund fehlender Flugpläne mussten die französischen Kampffjets zwei Tage lang am Boden beileiben.

Der Virus gelangte wahrscheinlich durch einen [USB-Stick](#) in das [Netzwerk](#).



News

Meldung vom 14.02.2009 18:15

[<< Vorige](#) | [Nächste >>](#)

Sie sind Gast

[Einloggen](#) | [Registrieren](#)

Hunderte Bundeswehr-Rechner von Conficker befallen vorlesen

Der seit Wochen weltweit grassierende Computer-Wurm "Conficker" hat mehrere hundert [Bundeswehr](#)-Rechner befallen. "Einzelne betroffene Dienststellen wurden vom Bundeswehr-Netzwerk getrennt, um eine weitere Ausbreitung der Schadsoftware zu verhindern", sagte ein Sprecher des [Bundesverteidigungsministeriums](#) am Samstag in Berlin. Derzeit gebe es aber keine weiteren Einschränkungen. Spezialisten eines Computer-Notfall-Teams der Bundeswehr und des Unternehmens BWI Informationstechnik GmbH hätten "Maßnahmen zur Entfernung der Schadsoftware und Wiederherstellung der vollen Funktionsfähigkeit der Computersysteme der Bundeswehr eingeleitet".

Suche

Im Browser einrichten

News

7-Tage-Alerts





13.02.2009 14:18



Zentrum für Informationstechnik der Bundeswehr
- Dezernat 11 -
Computer Emergency Response Team Bundeswehr
Kommerner Strasse 188
53879 Euskirchen

➤ Name / Alias:

CERTBw-Advisory 09/02: DRINGEND - Auftreten des Wurms Conficker/Downadup

Das Advisory ist nachgeordneten Dienststellen telefonisch bzw per Fax zu übermitteln

➤ Hintergrund:

In verschiedenen Dienststellen ist der als Conficker/Downadup bezeichnete Wurm aktuell aufgetreten.

Vor der zugrunde liegenden Schwachstelle und dem verfügbaren Patch hat CERTBw bereits im Advisory 08/16 gewarnt und auf das Update hingewiesen.

➤ Empfehlung:

CERTBw empfiehlt DRINGEND die angeführten Maßnahmen soweit noch erforderlich zu ergreifen. Ein Bereinigung bzw. Netztrennung von betroffenen Maschinen wird vor dem Wochenende



Studie IBM CERTBw

Überlegungen Aufbau IT-AmtBw

Anschlag World Trade Center NY

Ad hoc Aufstellung des CERTBw
durch IT-Direktor

Beginn der Ausbildung
(„Kernteam“)

Aufbau CERTBw
in Euskirchen

Verbessern
Fähigkeiten

12/2000

04/2001

11.09.2001

19.10.2001

03.12.2001

01.11.2002

2007



Das CERTBw ist für die zentrale Überwachung der IT-Sicherheit der Anteile im IT-System Bundeswehr (IT-SysBw), die das TCP/IP-Protokoll nutzen und nicht in der Betriebsverantwortung der BWI IT liegen, verantwortlich.



Lage-/Einsatzzentrum

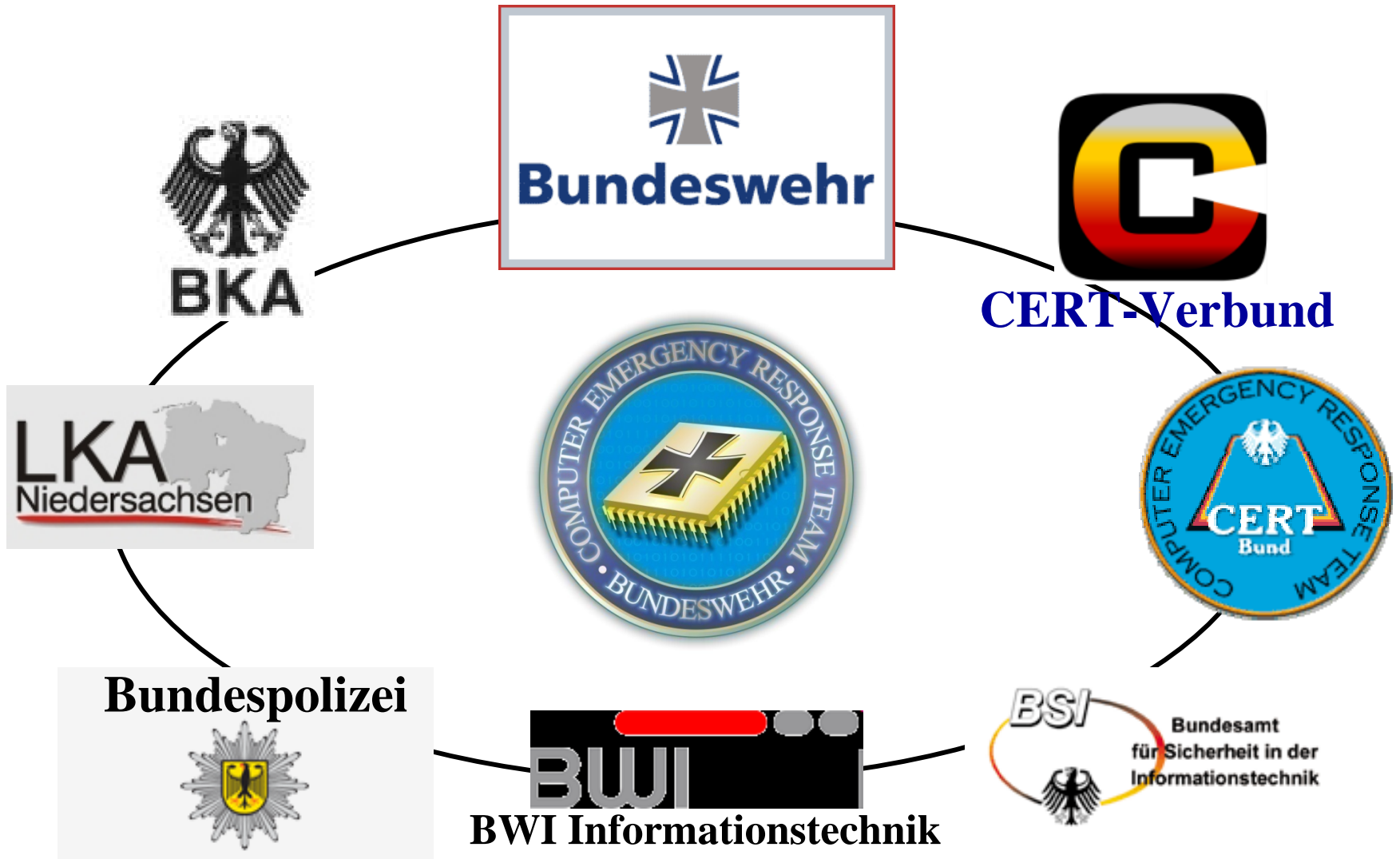
- **Koordinierung und Steuerung des Incident Managements mit Analyse, Bewertung und Auswertung von Vorfällen**
- **Durchführung von Maßnahmen zur Schadensbegrenzung und -Schadensbeseitigung**

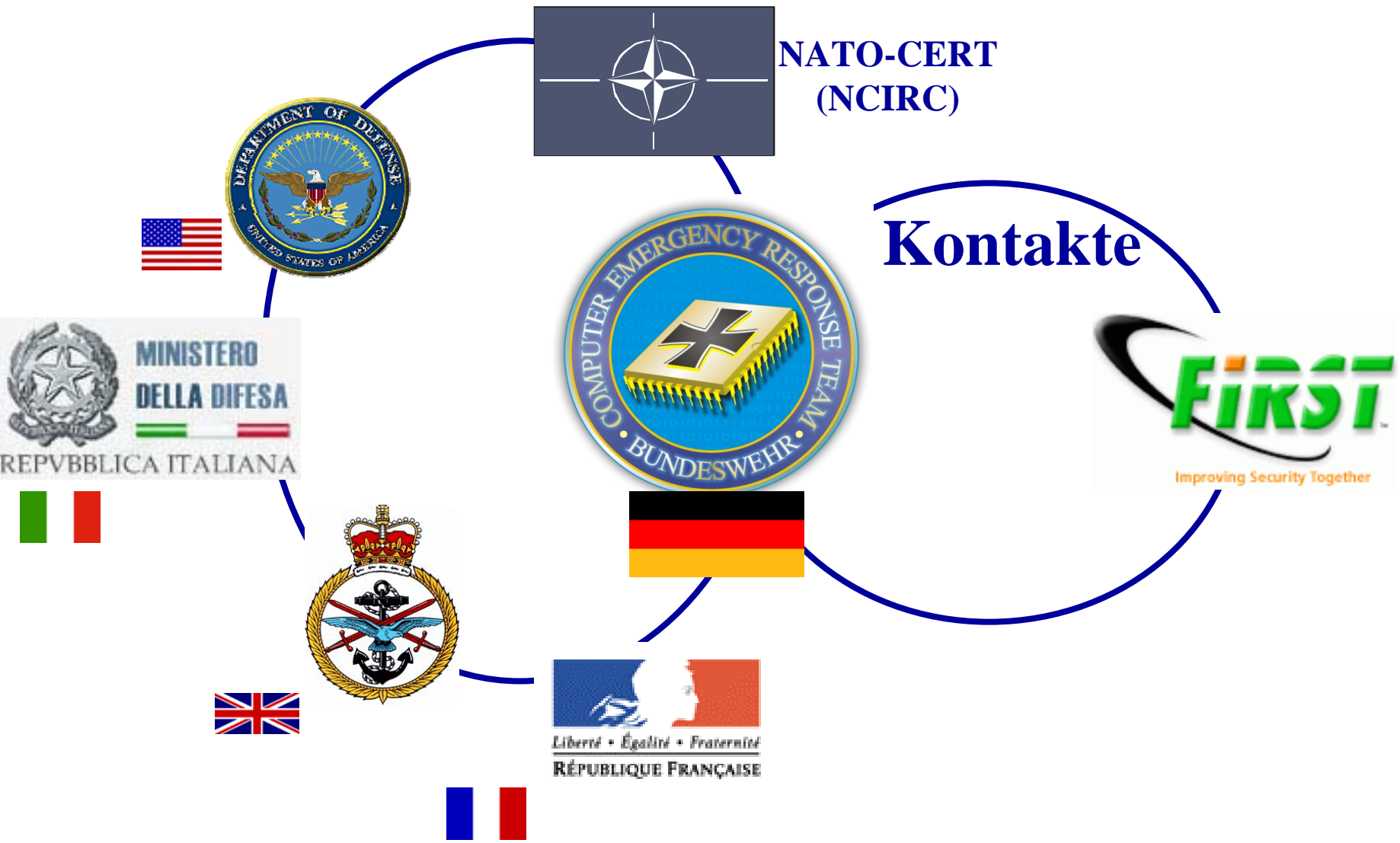
Incident Management Test Laboratory

- **Schwachstellenanalyse**
- **Entwicklung von Gegen- und präventiven Maßnahmen**
- **Elektronische Beweisführung**
- **Technische Unterstützung**

Network Security Operation Center (NSOC)

- **Alarmierung, Warnung und Reaktion bei Vorfällen**
- **Überwachung der zentralen Sicherheitsfunktion des IT-SystemBw**





Digital Storm (2003 – 2007)

Teilnehmer:

Mil. CERTs aus USA, GBR, FRA, ITA, DEU (CERTBw)

Ziel:

Erprobungen von Verfahren zur Zusammenarbeit und gemeinsamen Reaktion auf Cyber-Bedrohungen



NATO CD Ex „Cyber Coalition“

Leitung:

NATO

Teilnehmer:

- NCIRC, DEU (CERTBw), GRE, ITA, LIT, ESP, TUR, USA ?, GBR ?, FRA ?
- Mind. 7 weitere Nationen als Beobachter

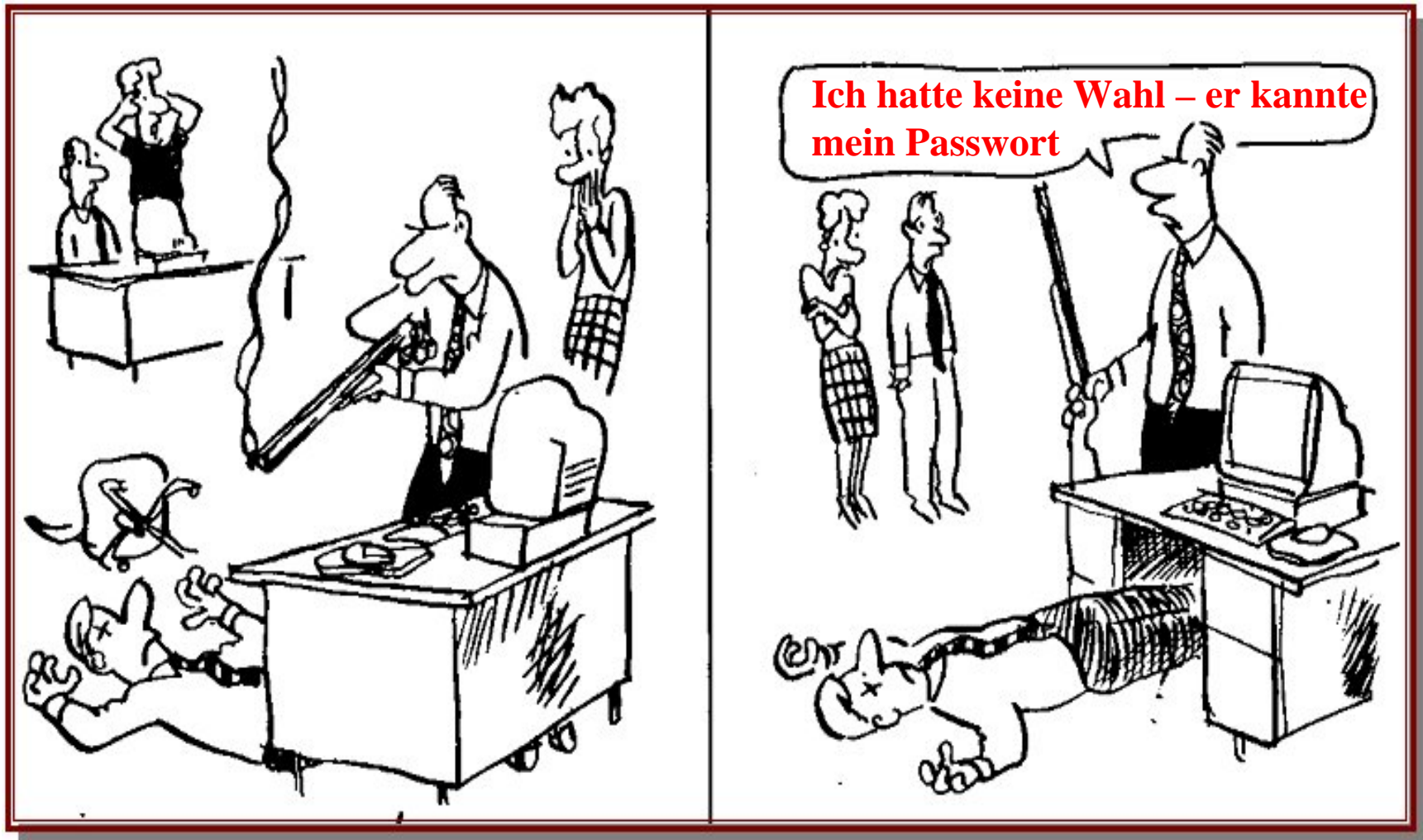
Ziel:

Erprobungen von Verfahren zur Entscheidungsfindung, Zusammenarbeit und gemeinsamen Reaktion auf Cyber-Bedrohungen

Durchführung:

Nov. 2009







**Bundesamt für Informationsmanagement
und Informationstechnik der Bundeswehr**

Oberstleutnant

Norbert Wildstacke

InfoOp / CNO / CIIP

**IT-AmtBw A6
Alte Heerstraße 149
D-56076 Koblenz**

**Tel.: +49 261/896-83 56
Fax: +49 261/896-83 65**

E-Mail: NorbertWildstacke@Bundeswehr.org