



eicar

DIE EICAR-TEST-DATEI: FELS IN DER BRANDUNG ODER ALTES EISEN?

22. DFN-KONFERENZ 25. Februar 2015

Tonke Hanebuth eicar@hanebuth.de www.eicar.org

EICAR

European Expert Group for IT Security

Gründung 1991

Idee

- European Institute for Computer Antivirus Research
- Koordination, Forschung, Bekämpfung von Malware
- Wissenschaftler, Entwickler, _Benutzer_ (Behörden, Unternehmen)
- Code of Conduct, Working Groups, Task Forces, Guides, Conference

Minimum Standard for Anti Malware Products

EICAR-TEST-DATEI

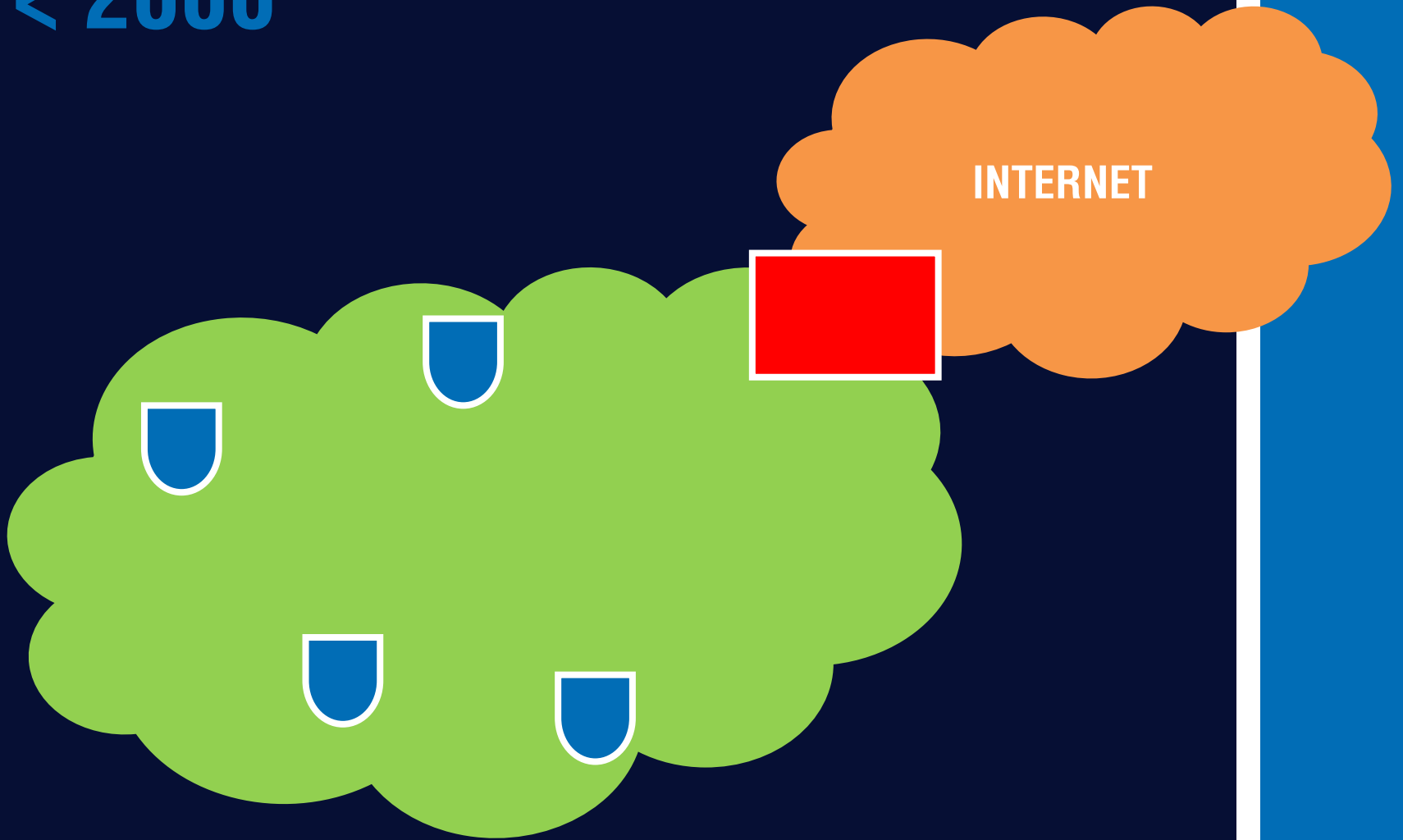
Funktioniert es? – jetzt hier bei mir
herstellerübergreifend

Reaktion wie auf Malware

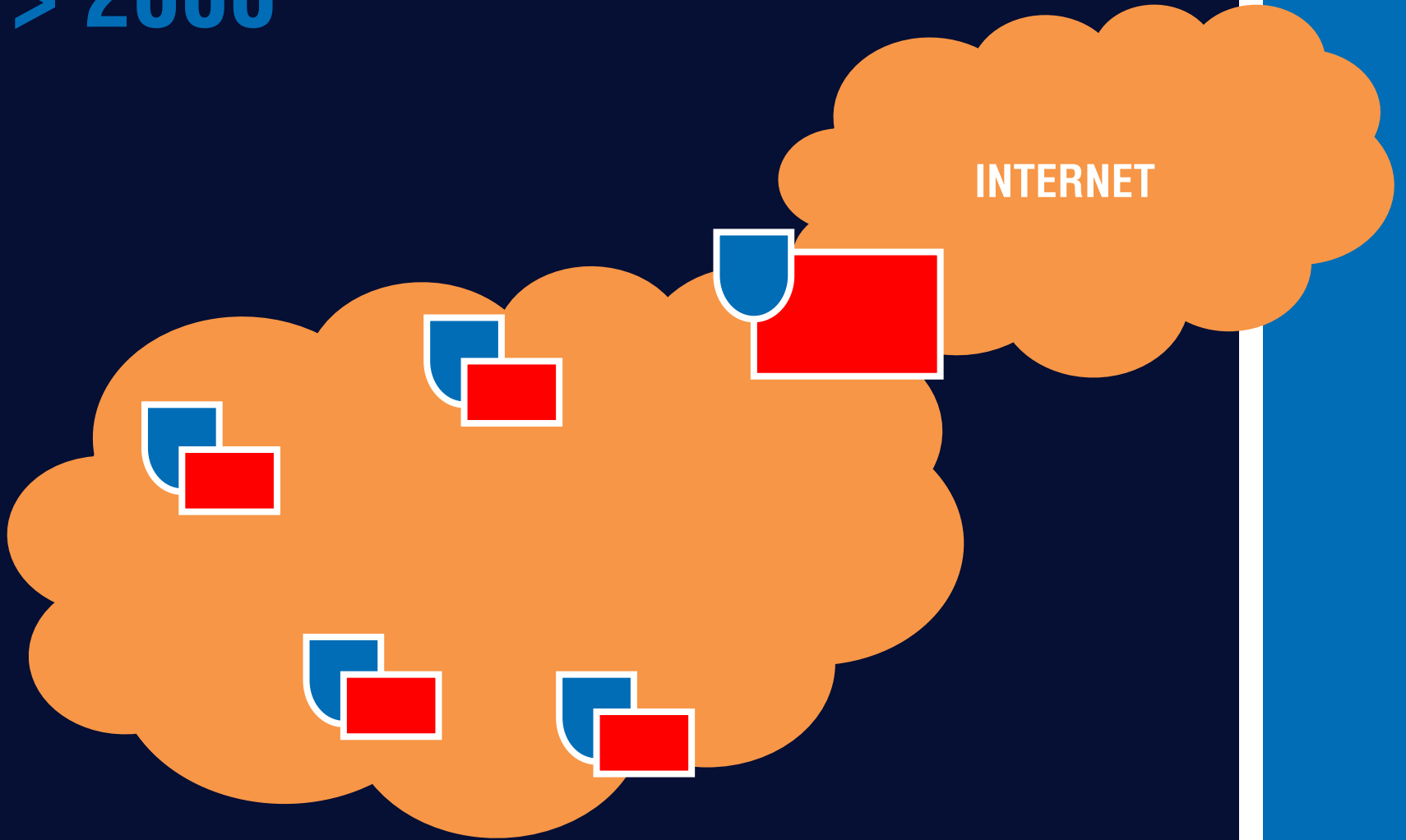
eicar.com

- > 20 Jahre alt

< 2000



> 2000



CYBER KILL CHAIN

DEFENSIBLE ACTIONS MATRIX

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Web Analytics	Firewall ACL				Firewall ACL
Weaponization	NIDS	NIPS				NIPS
Delivery	Vigilant User	Proxy Filter	Inline AV	Queuing		App-Aware Firewall
Exploitation	HIDS	Patch	DEP			Inter-Zone NIPS
Installation	HIDS	'chroot' Jail	AV			EPP
Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust Zones
Actions on Targets	Audit Logs	Outbound ACL	DLP	Quality of Service	Honeypot	Trust Zones

Best-Practice Defensible Actions Matrix Use Case [Partial]
nigesecurityguy.wordpress.com/tag/cyber-kill-chain

TEST FILE WORKING GROUP

Ziel

- Anpassung der EICAR-Testdatei an die aktuellen Anforderungen

Agenda Q2 2015

- Auswertung der Umfrage
- Workshop zur Planung des weiteren Vorgehens

UMFRAGE

The screenshot shows a web browser window displaying the EICAR Test File Working Group website. The browser's address bar shows the URL `www.eicar.org/133-0-Test-File-Working-Group.html`. The website header includes the EICAR logo and the text "EUROPEAN EXPERT GROUP FOR IT-SECURITY". A navigation menu contains links for "ABOUT US", "CONFERENCE", "PROJECTS", "ANTI-MALWARE TESTFILE", "PRESS", and "INFORMATION". A search bar is located on the right side of the navigation menu. The main content area features a sidebar with a "MEMBERS AREA" containing login fields for "Loginname" and "Password", and a "login" button. The main content area has a breadcrumb trail: "YOU ARE HERE > PROJECTS > TEST FILE WORKING GROUP". The main heading is "EICAR TEST FILE WORKING GROUP". Below the heading, the text states: "Our goal is the transformation of the EICAR test file into the contemporary environment." Under the heading "Project Objectives", it says: "We evaluate the need for new vendor independent tools to check security applications. If required we take care for provision of tools." Under the heading "The aims are not related to product rating or quality testing.", it says: "The aims are not related to product rating or quality testing." Under the heading "Schedule", it says: "documentation and publication of pre Conference 2014 November 16th workshop results". A red-bordered box highlights a section titled "WE ASK FOR YOUR HELP" with the text: "Dear visitor, we would be happy if you could help us to improve the EICAR test file by completing our survey. This important support takes 3 to 5 minutes only." Below this text is a link: "Start advanced survey".

Test File Working Group

www.eicar.org/133-0-Test-File-Working-Group.html

EUROPEAN EXPERT GROUP FOR IT-SECURITY

eicar

DOWNLOAD ANTI MALWARE TESTFILE

ABOUT US CONFERENCE **PROJECTS** ANTI-MALWARE TESTFILE PRESS INFORMATION

Searchword OK

YOU ARE HERE PROJECTS TEST FILE WORKING GROUP

EICAR TEST FILE WORKING GROUP

Our goal is the transformation of the EICAR test file into the contemporary environment.

Project Objectives

We evaluate the need for new vendor independent tools to check security applications. If required we take care for provision of tools.

The aims are not related to product rating or quality testing.

Schedule

documentation and publication of pre Conference 2014 November 16th workshop results

WE ASK FOR YOUR HELP

Dear visitor, we would be happy if you could help us to improve the EICAR test file by completing our survey. This important support takes 3 to 5 minutes only.

[Start advanced survey](#)



eicar

DANKE! FRAGEN?

22. DFN-KONFERENZ 25. Februar 2015

Tonke Hanebuth eicar@hanebuth.de www.eicar.org

LINKS

EICAR

- Test File Working Group & Fragebogen
 - www.eicar.org/133-0-Test-File-Working-Group.html
- Test File Documentation & Download
 - www.eicar.org/anti_virus_testfile.htm

GTUBE

- Generic Test for Unsolicited Bulk Email
- <http://spamassassin.apache.org/gtube/>