Offen

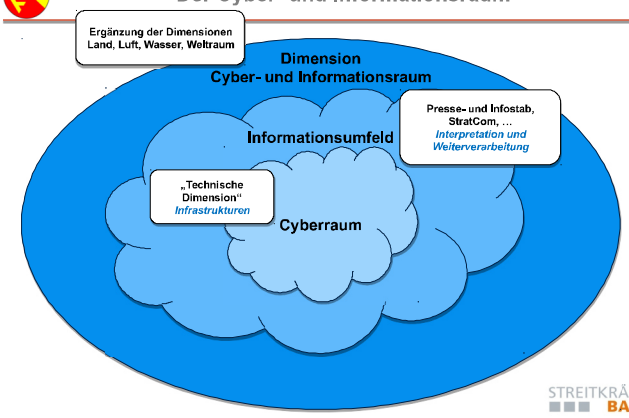
Führungsunterstützungskommando der Bundeswehr

FKpt Dr. Robert Koch
Dezernent Cyber
31.03.2017

Akademietag 2017
Cybersicherheit – Herausforderungen aus Sicht der Bundeswehr

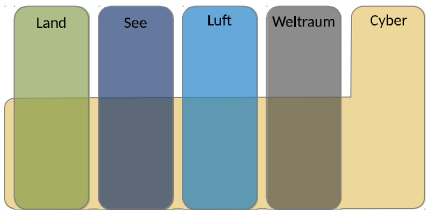
STREITKRÄFTE BASIS

Der Cyber- und Informationsraum



STREITKRÄFTE BASIS

Duale Rolle: Domäne & Enabler



STREITKRÄFTE BASIS

Herausforderungen für jeden Einzelnen

Beispiel: Hintergrund AV-Software

Antivirus Testergebnis: Die besten Antivirenprogramme 2016 im Vergleich

Der letzte Virenscanner Test wurde am **15.09.2016** durchgeführt. Alle Virenscanner haben wir mit älteren und neuen Schädlingen konfrontiert. Die Virenscanner wurden mit aktuellen Updates versorgt und hatten durchgehend eine funktionierende Internet-Verbindung. Mehr über das Testverfahren.

Rang	Virenscanner	Schutz ?	Handhabung ?	Belastung ?	Ausstattung ?	Preis ?
1	Bitdefender Internet Security 2017	100 %	10.0 Pkt.	10.0 Pkt.	10.0 Pkt.	49,95 Euro*
	*Entscheidest du dich für die 5-Jahres Lizenz, zahlst du nur 17,99 Euro/Jahr (einmalig 89,95 Euro). Bitdefender ist aktuell auch Testsieger bei den weltweit führenden Virenschutz-Testlaboren AV-TEST und AV-Comparatives.					
2	Kaspersky Internet Security 2017	96 %	9.0 Pkt.	9.0 Pkt.	10.0 Pkt.	49,95 Euro
3	Norton Security Deluxe	92 %	8.5 Pkt.	8.5 Pkt.	9.5 Pkt.	49,99 Euro
4	F-Secure Internet Security	88 %	7.0 Pkt.	8.0 Pkt.	7.0 Pkt.	49,90 Euro
5	Avira Internet Security	83 %	7.0 Pkt.	8.0 Pkt.	7.0 Pkt.	39,95 Euro
6	ESET Smart Security	82 %	8.5 Pkt.	7.0 Pkt.	9.5 Pkt.	34,95 Euro
7	Avast Free Antivirus	80 %	6.0 Pkt.	8.0 Pkt.	7.5 Pkt.	**Gratis**
8	G Data Internet Security					
9	Emsisoft Internet Security					
10	Avira Free Antivirus					
11	AVG Internet Security					
12	AVG Anti-Virus Free					
13	McAfee Internet Security					
14	Ad-Aware Pro Security					
15	Microsoft Windows Defender					

Ø Erkennungsrate im Test

Ältere Schädlinge: Ø 97.9%

Neue Schädlinge: Ø 80.9%

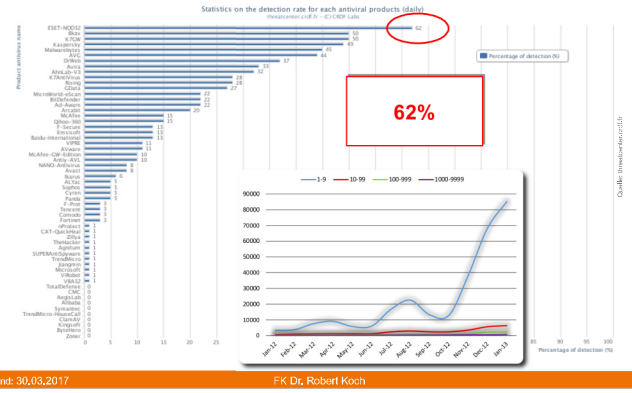
Genauere Betrachtung der Testergebnisse

Schädlinge	
Schädlings-Alter	Anzahl
Neue Schädlinge	100
Ältere Schädlinge	900
Summe	1000

431 Mio. neue Schadprogramme 2015

„0,0002%“

Reviewed



Aktuelles Beispiel

Overview

Our research team has uncovered a new Zero-Day attack for taking full control over major antiviruses and next-generation antiviruses. Instead of hiding and running away from the antivirus, attackers can now directly assault and hijack control over the antivirus.
The attack begins when the attacker injects code into the antivirus by exploiting a new Zero-Day vulnerability. Once inside, the attacker can fully control the antivirus. We named this attack DoubleAgent, as it turns your antivirus security agent into a malicious agent, giving an illusion that the antivirus protects you while actually it is abused in order to attack you.

DoubleAgent exploits a 15 year old vulnerability which works on all versions of Microsoft Windows, starting from Windows XP right up to the latest release of Windows 10. The sad, but plain fact is that the vulnerability is yet to be patched by most of the antivirus vendors and could be used in the wild to attack almost any organization that uses an antivirus. Once the attacker has gained control of the antivirus, he may command it to perform malicious operations on behalf of the attacker.
Because the antivirus is considered a trusted entity, any malicious operation done by it would be considered legitimate, giving the attacker the ability to bypass all the security products in the organization.

The attack has been tested and proven on all the major antiviruses as well as of all versions of Microsoft Windows. The attack was reported to all the major vendors which approved the vulnerability and are currently working on finding a solution and releasing a patch.

Herausforderungen

Umgang mit Daten…

- Beispiel Erschießung Geheimdienstagent Nicola Calipari
- Untersuchungsbericht in Word geschwärzt, PDFMaker 6.0 Export

5. (U) Rhino Bus Run TTP Background Information

(U) Since October 20
Most of the contacts wer
assessment of the Coalit

[redacted]

5. (U) Rhino Bus Run TTP Background Information

(U) Since October 2004, there had been significant insurgent contact on Route Irish. Most of the contacts were RPGs, SAF, IEDs, and VBIEDs. These attacks prompted a re-assessment of the Coalition's responses for operations along Route Irish.

(S//NF) Route Irish is the primary route to BIAP for U.S. Embassy personnel, and there was routinely at least one convoy each day. Rhino buses (armored buses) were procured to provide better protection for passengers. Additionally, a series of briefings and plans were developed to address the insurgent situation along Route Irish. The result was the Rhino Bus Run Program. (Annex 65C).

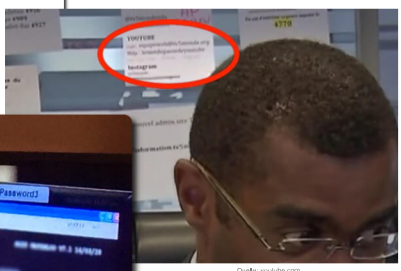
[redacted](S//NF) Under the Rhino Bus Run Program, 1-76 FA escorts two or three Rhino armored buses and one or two baggage trucks to and from the Embassy staging area in the International Zone and the BIAP passenger terminal twice nightly, seven days a week. Each run consists of up to 65 escorted passengers. This is the standard TTP 1-76 FA learned during the Right Seat/Left Seat Ride program conducted by 2-82 FA as part of Relief in Place operations. 1-76 FA's higher headquarters, Fourth Brigade, coordinates attack helicopter support to conduct route reconnaissance ahead of the convoy and Close Air Support in the event of an attack. (Annex 59C).

STREITKRÄFTE BASIS

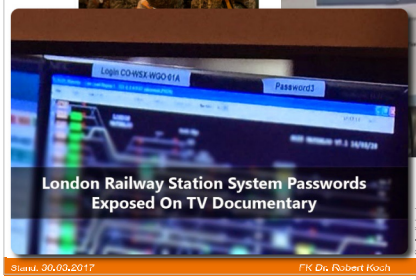
Zufall, Background & 23 MP++

Insurgents Used Cell Phone Geotags to Destroy AH-64s in Iraq

Quelle: defensetech.org



Quelle: youtube.com



London Railway Station System Passwords Exposed On TV Documentary

Quelle: theguardian.com

STREITKRÄFTE BASIS

Bedeutung Informationsraum

DIGITALE MANIPULATION

Wie Social Bots den Brexit verursachten

Wird die Demokratie im Zeitalter der Digitalisierung b
Monaten warnten neun Wissenschaftler in einem ex
publizierten Digital-Manifest eindringlich vor Gefahre
Verhaltenssteuerung auf Grundlage digitaler Techno
Widerhall? Ein Interview mit dem Sozialwissenschaf
Experten Dirk Helbing.

Quelle: spektrum.de

Einsatz in Litauen

Nato vermutet Russland hinter Fake-News-Kampagne gegen Bundeswehr

Die Bundeswehr ist bei ihrer Baltikum-Mission Ziel einer perfiden Kampagne geworden. Nach SPIEGEL-Informationen wurden offenbar aus Russland Gerüchte über eine angebliche Vergewaltigung durch deutsche Soldaten gestreut.

Von Matthias Gebauer

Bundeswehr-Soldaten auf dem Weg nach Litauen

Quelle: spiegel.de

STREITKRÄFTE BASIS

Vernetzte Operationsführung

Bundeswehr

Effizienz-steigerung

Wirküberlegenheit

Führungs-überlegenheit

Informations-überlegenheit

Situational Awareness

Verbesserte Vernetzung

STREITKRÄFTE BASIS

Sicherheit von Waffensystemen…

Bundeswehr

Defence Secretary announces major cyber investment

From: Ministry of Defence and The Rt Hon Sir Michael Fallon MP
First published: 20 October 2016

The UK will invest up to £265m to boost the defence of military cyber systems, the Defence Secretary has announced.

Defence Secretary Michael Fallon spoke at the second RUSI Cyber Symposium. Crown Copyright.

Michael Fallon said the investment, which supports the new Cyber Vulnerability Investigations (CVI) programme, will help the MOD better understand cyber risks.

Speaking at the second International Cyber Symposium Mr Fallon said it will also help the MOD ensure that resilience to cyber-attack is built-in when buying equipment in future.

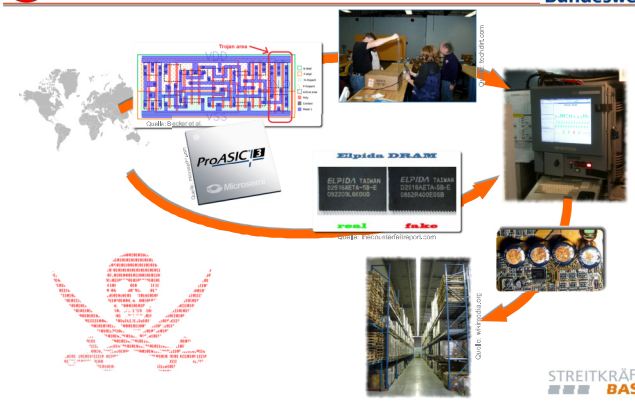
Defence Secretary Michael Fallon said:

" Cyber-attack is one of the greatest challenges to our security. It's crucial we use our increasing defence budget to stay ahead and investing in this programme will help us protect against these threats."

STREITKRÄFTE BASIS

Auszug aus dem Bedrohungsspektrum…

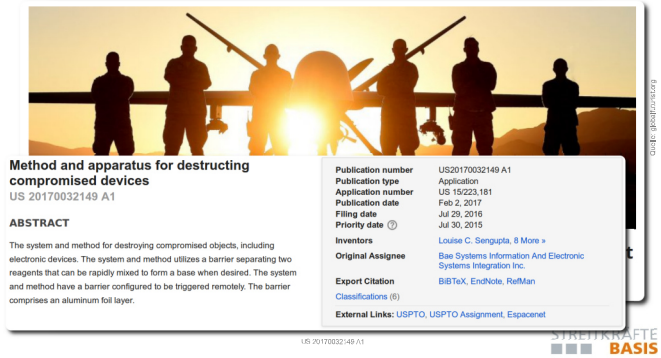
Bundeswehr



STREITKRÄFTE BASIS

Stand Drohnen und 3d-Druck

Entwicklung von „Vampire Drones“



Method and apparatus for destructing compromised devices
US 20170032149 A1

ABSTRACT

The system and method for destroying compromised objects, including electronic devices. The system and method utilizes a barrier separating two reagents that can be rapidly mixed to form a base when desired. The system and method have a barrier configured to be triggered remotely. The barrier comprises an aluminum foil layer.

Publication number	US20170032149 A1
Publication type	Application
Application number	US 15/223,181
Publication date	Feb 2, 2017
Filing date	Jul 29, 2016
Priority date	Jul 30, 2015
Inventors	Louise C. Sengupta, 8 More »
Original Assignee	Bae Systems Information And Electronic Systems Integration Inc.
Export Citation	BiBTeX, EndNote, RefMan
Classifications (6)	

External Links: USPTO, USPTO Assignment, Espacenet

US 20170032149 A1

Entwicklungen im Bereich Speicher

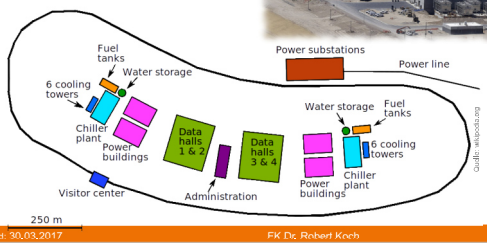
Bedeutung…

Utah Data Center

(Vernünftige) Schätzung 2013

~ 3..12 Exabyte

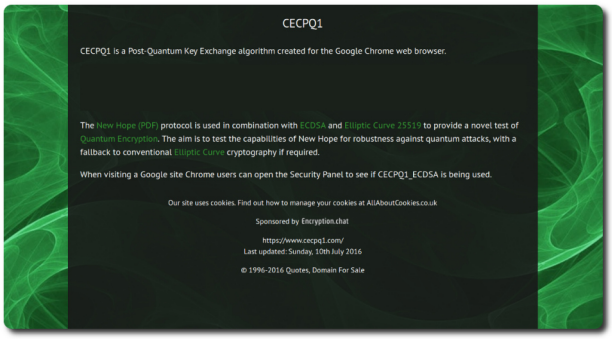
Quelle: wikipedia.org



Quelle: wikipedia.org

STREITKRÄFTE BASIS

Stand Quantenrechner



CECPQ1

CECPQ1 is a Post-Quantum Key Exchange algorithm created for the Google Chrome web browser.

The New Hope (PDF) protocol is used in combination with ECDSA and Elliptic Curve 25519 to provide a novel test of Quantum Encryption. The aim is to test the capabilities of New Hope for robustness against quantum attacks, with a fallback to conventional Elliptic Curve cryptography if required.

When visiting a Google site Chrome users can open the Security Panel to see if CECPQ1_ECDSA is being used.

Our site uses cookies. Find out how to manage your cookies at AllAboutCookies.co.uk

Sponsored by Encryption.chat

https://www.cecpq1.com/
Last updated: Sunday, 10th July 2016

© 1996-2016 Quotes, Domain For Sale

Quelle: cecpq1.com

STREITKRÄFTE BASIS

Entscheid BM'in der Verteidigung Oktober 2016

Tagesbefehl 05. Oktober 2016

- **Erster Meilenstein** des erweiterten Aufbaustabs CIR erreicht
- Einrichtung einer neuen **Abteilung Cyber/IT im BMVg in BERLIN und BONN** mit **Klaus-Hardy Mühleck** als Abteilungsleiter CIT und Ressort Chief Information Officer.
- Weichenstellung für **stärker IT-getriebene Modernisierung** und Aufwertung CIR zu einer **eigenständigen militärischen Dimension.**

STREITKRÄFTE BASIS

Startschuss für CIR

STREITKRÄFTE BASIS

Cyberhygiene

„If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.“

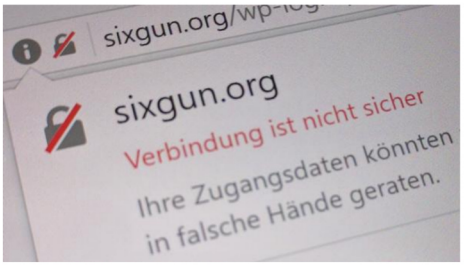
– Bruce Schneier

STREITKRÄFTE BASIS

DIE Herausforderung… Fachkräfte (fort.')

Unsicheres Log-in-Feld: Webseiten-Betreiber beschwert sich bei Firefox über Warnung

21.03.2017 11:56 Uhr – Fabian A. Scherschel vorlesen



Der Firefox-Browser warnt seit einiger Zeit vor Passwortfeldern, deren Inhalte unverschlüsselt an den Server übermittelt werden. Ein Admin will das allerdings nicht hinnehmen – seine Systeme seien sicher, seit über 15 Jahren.

STREITKRÄFTE BASIS

Forschungsinstitut CODE

der Bundeswehr
Universität München

RC CODE Research Center Cyber Defence
Universität der Bundeswehr München

Startschuss für ZITiS

400 Stellen bis 2022 in der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) in München geplant

Quelle: www.chip.de

STREITKRÄFTE BASIS

Cybersicherheit

- Jeder Einzelne muss sich seiner Rolle…
- … und der Cybergefahren bewusst sein!
- **Cyberhygiene & Awareness**

Bundeswehr

- Cyber als Enabler und Operationsraum
- Hochkomplexes Gesamtsystem
- Rasante technische Weiterentwicklung
- **Faktor Mensch bleibt schwächstes Glied**
- **Cyberhygiene, Awareness, umfassende Sich'kenntnisse**

Offen

Führungsunterstützungskommando der Bundeswehr

FKpt Dr. Robert Koch
Dezernent Cyber
31.03.2017

Akademietag 2017
Cybersicherheit – Herausforderungen aus Sicht der Bundeswehr

STREITKRÄFTE BASIS