3. Wirtschaftsschutztag Sachsen-Anhalt

Neue Risiken, neue Bedrohungen?

IHK MAGDEBURG

SACHSEN-ANHALT
Ministerium für
Inneres und Sport

#moderndenken

Vorwort

Jochen Hollmann
Leiter der Abteilung Verfassungsschutz im Ministerium für Inneres und Sport des Landes Sachsen-Anhalt

Am 6. November 2019 fand bereits zum dritten Mal in Zusammenarbeit mit der Industrie- und Handelskammer (IHK) Magdeburg der Wirtschaftsschutztag Sachsen-Anhalt mit einem breitgefächerten und qualifizierten Programm statt. Die überregionale Expertise repräsentierten das Bundesamt für Sicherheit in der Informationstechnik und das Bundesamt für Verfassungsschutz mit ihren Fachvorträgen. Referenten aus Sachsen-Anhalt wiesen auf die Risiken und Schutzmöglichkeiten im Zuge der weiteren Internationalisierung der Wirtschaftsbeziehungen hin. Die breite Palette landeseigener Expertise spiegelte sich in den Fachvorträgen zur Detektion von Malware, zur Identifizierung von Produkten, die auf Grund ihrer Betriebssysteme Ausspähungsrisiken mit sich bringen, und über die Forschung zur IT-Security an Sachsen-Anhalts akademischen Einrichtungen.

Zwischen den Vortragsblöcken am Vormittag und am Nachmittag fand erstmals eine Networkingbörse mit Wirtschaftsschutzakteuren statt, die die Vertreterinnen und Vertreter der Unternehmen und Behörden zu individuellen Gesprächen mit den Sicherheitsbehörden und zum Netzwerken nutzten.

Wirtschaft und Wissenschaft, Bundesbehörden und Landesinstitutionen sind sich einig, dass neben die technischen Cybersecurity-Maßnahmen die Sensibilisierung der Mitarbeiter treten muss. Das Verhalten der Mitarbeiter aller Sektoren stellt im Zusammenhang mit analoger und digitaler Kommunikation den Schlüssel zu mehr IT-Security dar. Dies gilt besonders in Zeiten, in denen eine zunehmende Anzahl von Mitarbeiterinnen und Mitarbeitern im Homeoffice arbeitet.

Insofern kann der 3. Wirtschaftsschutztag mit rund 120 Teilnehmenden als Erfolg bezeichnet werden. Mein Dank richtet sich an die IHK Magdeburg, die die Veranstaltung professionell vorbereitet und mitgestaltet hat.

Natürlich dürfen wir hier nicht stehenbleiben. Unternehmen sind täglich Risiken ausgesetzt und Optimierung ist möglich. Für sachsen-anhaltische Unternehmen stehen im Bereich der Mitarbeitersensibilisierung kommerzielle und nicht-kommerzielle Angebote bereit. Zu diesen gehören die Angebote des Wirtschaftsschutzes der Verfassungsschutzbehörden. Nutzen Sie diese!
Der Tagungsband dient insoweit nicht nur der Dokumentation und der Rekapitulation des 3. Wirtschaftsschutztages, sondern will auch das Bewusstsein für die Risiken schärfen und aufzeigen, wie man sich schützen kann.

Ergänzend darf ich auf die Internetseite des Verfassungsschutzes Sachsen-Anhalt unter: www.mi.sachsen-anhalt.de/verfassungsschutz mit weiteren für die Firmensicherheit relevanten Informationen verweisen.

Abschließend möchte ich darauf hinweisen, dass die Beiträge der Referentin und Referenten deren Auffassungen zum Ausdruck bringen.

Magdeburg, im Juli 2020

Inhalt

Begrüßung

Klaus Olbricht
Präsident der Industrie- und Handelskammer Magdeburg

Es gilt das gesprochene Wort!

Sehr geehrter Frau Staatssekretärin,

sehr geehrte Referenten der Veranstaltung,

meine sehr verehrten Damen,

sehr geehrte Herren,

im Namen der Industrie- und Handelskammern Magdeburg und des Ministeriums für Inneres und Sport des Landes Sachsen-Anhalt heiße ich Sie herzlich willkommen zu unserem 3. Wirtschaftsschutztag des Landes Sachsen-Anhalt hier im Tagungszentrum der IHK Magdeburg.

Es ist mir eine große Freude, Sie, sehr geehrte Staatssekretärin Frau Dr. Zieschang, als Schirmherrin dieser Veranstaltung begrüßen zu dürfen und gemeinsam mit Ihnen den Wirtschaftsschutz wieder einmal mehr in den Fokus der Öffentlichkeit zu rücken.

Vor einigen Jahren sprachen wir über Digitalisierung im Zusammenhang mit Industrie 4.0 noch als eine Art Revolution. Im Jahr 2019 ist es eine Selbstverständlichkeit geworden. Das Internet startete 1991 mit dem ersten kommerziellen Internetprovider seinen Siegeszug außerhalb der Universitäten. Knapp 30 Jahre später nutzen allein in Deutschland täglich 50 Millionen Menschen für knapp 2,5 Stunden das Internet.

Und auch unsere Kühlschränke, Waschmaschinen und Autos nutzen ihr eigenes Internet of Things – also Internet der Dinge.

Wie kurz der Zeitraum für diesen Wandel war, ist auch ein Beleg dafür, in welcher Geschwindigkeit unsere technologische Entwicklung voranschreitet. So schnell auch die technische Entwicklung voranschreitet, bleibt es im Tagesgeschäft dennoch häufig schwierig, in gleicher Geschwindigkeit Anpassungsprozesse in den Betrieben anzustoßen und umzusetzen. Viele Fragen tauchen auf: Beispielsweise zum konkreten Nutzen durch eine vernetzte Produktion, zur Datensicherheit oder wie die Mitarbeiterinnen und Mitarbeiter in den Prozess mit eingebunden werden können.

Auch im Außenverhältnis müssen Geschäftspartner, Kunden und Zulieferer in die im Zuge der Digitalisierung entstehenden Veränderungen einbezogen werden. Denn bei Digitalisierung in der Wirtschaft geht es um die Vernetzung weit über die Fertigungsprozesse im eigenen Unternehmen hinaus. Es kommt vielmehr zu Verschiebungen in der gesamten Wertschöpfungskette, welche nicht länger in ferner Zukunft liegen.

Ein wesentlicher Bestandteil der digitalisierten Welt ist das Thema Sicherheit. Bei der Entwicklung ist es wichtig, dass nicht unzureichende Daten- und Informationssicherheit nicht zum Hemmnis

werden. IT-Sicherheit muss bei der Digitalisierung mit eingeplant werden.

Und wer von Ihnen am heimischen PC bereits einen Virenbefall hatte, der kennt das kompromittierende Gefühl, die Hoheit über die eigenen Daten verloren zu haben. Auf die Firma übertragen vervielfacht sich dieses Gefühl noch.

Die Unternehmensstruktur in Sachsen-Anhalt ist geprägt durch klein- und mittelständische Unternehmen. Diese Betriebe sind oft darauf angewiesen, sich durch die Schaffung von Innovationen und Spitzentechnologien einen technologischen Vorsprung zu erarbeiten.

Sachsen-Anhaltische Unternehmen besitzen dem zufolge sehr großes Potential und agieren in europäischem und internationalem Umfeld. In diesem Sinne sollte auch hier das Sicherheitsbewusstsein vergrößert werden.

Klein- und mittelständische Unternehmen verfügen aber häufig nicht über das entsprechende Problem- oder Gefahrenbewusstsein und in Folge dessen auch in weit geringerem Maße als Großunternehmen über entsprechende Schutzmechanismen. Sie sind deshalb besonders häufig Opfer verschiedenster Delikte aus dem großen Bereich des „Cybercrime“.

Ebenfalls nicht aus dem Blick zu verlieren ist neben dem Schutz der Informations- und Kommunikationssysteme auch der Schutz und die besondere Aufmerksamkeit und Bedeutung des Faktors Mensch. Wer Mitarbeiter im Rahmen der Ausweitung seiner Geschäftstätigkeit ins Ausland entsendet, muss rechtlich und kulturell gut vorbereitet und sich der zu erwartenden Risiken und rechtlichen Verpflichtungen bewusst sein. Der Schutz der Mitarbeiter und gleichsam der Schutz der wirtschaftlichen Unternehmensinteressen ist ebenfalls ein nicht außer Acht zu lassendes Thema des Wirtschaftsschutzes.

Vor diesen Hintergrund stellen sich also viele Fragen:

Wie sicher ist mein Unternehmen?

Welchen Gefahren und Bedrohungen ist mein Unternehmen in Ausland ausgesetzt?

Wie steht es dabei um die IT-Sicherheit in meinem Unternehmen?

Die folgenden Vorträge und Unternehmensberichte werden Ihnen die ein oder andere Antwort geben können, um die weiteren Schritte auf dem Weg zu einer sicheren Digitalisierung im eigenen Unternehmen in Angriff zu nehmen.

Meine sehr geehrten Damen und Herren,

wie ich Ihnen in meinen kurzen Ausführungen bereits aufzeigen wollte, bietet Ihnen der heutige Wirtschaftsschutztag ein vielfältiges und facettenreiches Programm. Ich wünsche uns allen eine spannende, erkenntnisreiche Veranstaltung und danke Ihnen für die Aufmerksamkeit.

Sehr geehrte Staatssekretärin Frau Dr. Zieschang, Sie haben das Wort.

Grußwort

Dr. Tamara Zieschang

Staatssekretärin im
Ministerium für Inneres und Sport
des Landes Sachsen-Anhalt

(bis Dezember 2019)

Es gilt das gesprochene Wort!

Meine sehr geehrten Damen und Herren,

ich begrüße Sie herzlich zur Wirtschaftsschutztagung der Industrie- und Handelskammer Magdeburg und der Verfassungsschutzbehörde Sachsen-Anhalt. Mein besonderer Dank richtet sich an den Hausherrn, Herrn Kammerpräsident Klaus Olbricht, dass wir hier im großen Saal der IHK Magdeburg gemeinsam den 3. Wirtschafts-schutztag Sachsen-Anhalt durchführen können. Herzliche Grüße darf ich Ihnen von Herrn Minister Holger Stahlknecht überbringen.

Ich freue mich, den Präsidenten des Amtes für Verfassungsschutz Thüringen, Herrn Kramer, und den Kommandeur des Landeskommandos Sachsen-Anhalt Oberst Halvor Adrian begrüßen zu können. Des Weiteren darf die Ständige Vertreterin des Generalstaatsanwalts, die Leitende Oberstaatsanwältin Frau Dr. Wieck-Noodt, herzlich begrüßen.

In diesem Monat feiern wir 30 Jahre Mauerfall. Am 9. November vor 30 Jahren begann der Sturz der letzten Diktatur auf deutschem Boden. Mit dem Prozess, der zur deutschen Einheit führte, gründeten sich in allen ostdeutschen Bundesländern Verfassungsschutzbehörden, die den Auftrag haben, unsere Demokratie präventiv vor ihren Feinden zu schützen. Heute gibt es zwar keine Machtblöcke mehr, die sich hochgerüstet in der Mitte Europas gegenüberstehen. Dennoch müssen die Verfassungsschutzbehörden feststellen, dass es nach wie vor Spionageaktivitäten fremder Nachrichtendienste gegen die Bundesrepublik Deutschland gibt. Neben der klassischen Spionage nutzen die Dienste fremder Staaten neue Instrumente wie elektronische Angriffe oder Einflussmaßnahmen mit erheblichem Schadenspotenzial für die Wirtschaft.

Zu den Schäden in Folge von digitaler Wirtschaftsspionage, Sabotage und Datendiebstahl berichtete der BITKOM-Verband in einer Studie zum Wirtschaftsschutz in der Industrie im letzten Jahr, dass bei konservativer Schätzung von einem Gesamtschaden in Höhe von 43,4 Mrd. Euro auszugehen ist.

In der vom Bundeskriminalamt in Auftrag gegebenen Studie „Wirtschaftsspionage und Konkurrenzausspähung“ (WISKOS), die ebenfalls 2018 erschien, stellte das Freiburger Max-Planck-Institut fest, dass die Digitalisierung nicht nur große Potenziale mit sich bringt, sondern auch neue Herausforderungen gerade auf dem Gebiet des Informationsschutzes. Es wird befürchtet, dass mit der rasanten Entwicklung ein schneller Transfer auch komplexer, technologischer Informationen möglich werden wird, der die traditionellen Know-how-Vorsprünge gerade im Bereich der kleinen und mittleren Unternehmen schneller schwinden lassen könnte als bisher. Im Ergebnis hat die Untersuchung gezeigt, dass die innerbetriebliche Prävention von Wirtschaftsspionage erfolgversprechend den Abfluss von Know-how verhindern kann.

Ziel dieser Veranstaltung heute ist deshalb, den Informationsraum zu öffnen und zu zeigen, dass die hier präsentierten Informationen auch für Ihre Unternehmen abrufbereit zur Verfügung stehen, um Unternehmensmitarbeiter in Sachen Sicherheit zu schulen.

Einer der Autoren der BITKOM-Studie, Herr Dr. Dan Bastian Trapp vom Bundesamt für Verfassungsschutz, und sein Kollege, Herr Christoph Feck, werden uns daher sowohl über Wirtschaftsspionage fremder Nachrichtendienste als auch über die Abwehr von Cyberangriffen fremder Nachrichtendienste berichten.

Am 17. Oktober erschien der neueste Bericht des Bundesamtes für Sicherheit in der Informationstechnik „Die Lage der IT-Sicherheit in Deutschland 2019“, eine lohnenswerte Lektüre, die mit „immer mehr, immer öfter“ zutreffend zusammengefasst werden kann. Dem Lagebericht nach haben Angriffe mit Ransomware, also erpresserischer Verschlüsselungssoftware, zugenommen, Produktionsausfälle in der Wirtschaft waren zu beklagen, ebenso erhebliche Beeinträchtigungen von Krankenhäusern und kommunalen Einrichtungen. Die kritischen Infrastrukturen erstatteten gemäß ihrer gesetzlichen Pflicht öfter Anzeige über kritische IT-Angriffe bzw. –ausfälle als im Berichtszeitraum zuvor. Ich freue mich, dass Frau Ariane Steinke vom BSI-Regionalbüro Nord in Hamburg uns dazu die Sicht ds BSI vortragen wird.

Mit der AV Test GmbH existiert in Magdeburg ein hochspezialisiertes Unternehmen, das in seinen Datenbanken über 800 Millionen Viren, Würmer und andere Schadsoftware speichert. Sie hat es sich zur Aufgabe gemacht, Antivirensoftware für PCs, Smartphones und vieles anderes mehr zu testen und sorgt so für eine einzigartige Transparenz auf dem Cybersecurity-Markt.

Ich kann heute Herrn Olaf Pursche, den Chief Communications Officer (CCO) des Unternehmens begrüßen, der einen Titel gewählt hat, der fast schon eine Inhaltsangabe ist. Er wird uns über Malware-Attacken, Tests von Gegenständen aus dem Internet der Dinge (IoT) berichten und eine Lagebestimmung aus Unternehmenssicht vornehmen.

Vor der Mittagspause wird uns der IT-Unternehmer und Vorsitzende der IT- und Multimediaindustrie-Verbandes Sachsen-Anhalts, Marco Langhof, Digitalisierungsprobleme aus seiner Sicht schildern. Als Anbieter intelligenter Softwarelösungen und gleichzeitig als Verbandsvertreter verfügt er über eine Fülle von Erfahrungen zum Thema Digitalisierung, die er als Mitglied des Digitalisierungsbeirates des Landes Sachsen-Anhalt in die Landesstrategie einbringt.

Information schadet nur dem, der sie nicht hat. Daher bieten wir Ihnen beim heutigen Wirtschaftsschutztag Sachsen-Anhalt nach dem ersten Vortragsteil zur Mittagszeit ein aktives Element an: Die Informations- und Networking-Börse. Die Börse bietet Ihnen die Möglichkeit, Ihren konkreten Informationsbedarf zu vervollständigen und auch Fragen rund um die Sicherheit Ihres Unternehmens oder Ihrer Behörde zu stellen. Dazu stehen Ihnen neben den Referenten weitere Experten zur Verfügung, um mit Ihnen die individuellen Belange ihres Unternehmens, ihres Instituts oder ihrer Behörde zu besprechen. Sofern Sie es wünschen, können Sie gerne auch vertraulich in einem der gekennzeichneten Besprechungsräume mit dem Experten ihres Vertrauens diskutieren.

Die Feinde der offenen Gesellschaft, die Datendiebe und Cybersaboteure, seien sie nun in fremden Nachrichtendiensten, in der organisierten Kriminalität, in virtuellen Hackerzirkeln oder in Ihrem Konkurrenzunternehmen, nutzen die Möglichkeiten der neuesten Internettechnologien und das Darknet für ihre

schädlichen Zwecke. Cybersicherheit bedarf der Forschung, ihre Mittel und Methoden müssen an den Herausforderungen wachsen. Im Anschluss an die Networking-Börse können Sie erfahren, welche Fortschritte die Cybersecurity-Bemühungen im Bereich der akademischen Forschung in Sachsen-Anhalt gemacht haben. Hierzu werden wir Herrn Professor Hermann Strack von der Hochschule Harz hören, der Teil des CyberSecurity-Verbunds Sachsen-Anhalt ist.

In diesem Sinne wünsche ich uns eine interessante und bereichernde Wirtschaftsschutztagung, die gute Impulse vermittelt, damit Sie die Informationssicherheit Ihres Unternehmens oder Ihrer Behörde im Zeitalter der Digitalisierung befördern können.

„Gefahren erkennen, IT-Sicherheit schaffen:
Von Malware-Angriffen, mobiler Sicherheit & IoT-Attacken, Lagebestimmung anhand aktueller Tests des AV-TEST Institut“

Olaf Pursche
Chief Communictions Officer (CCO)
AV Test GmbH, Magdeburg

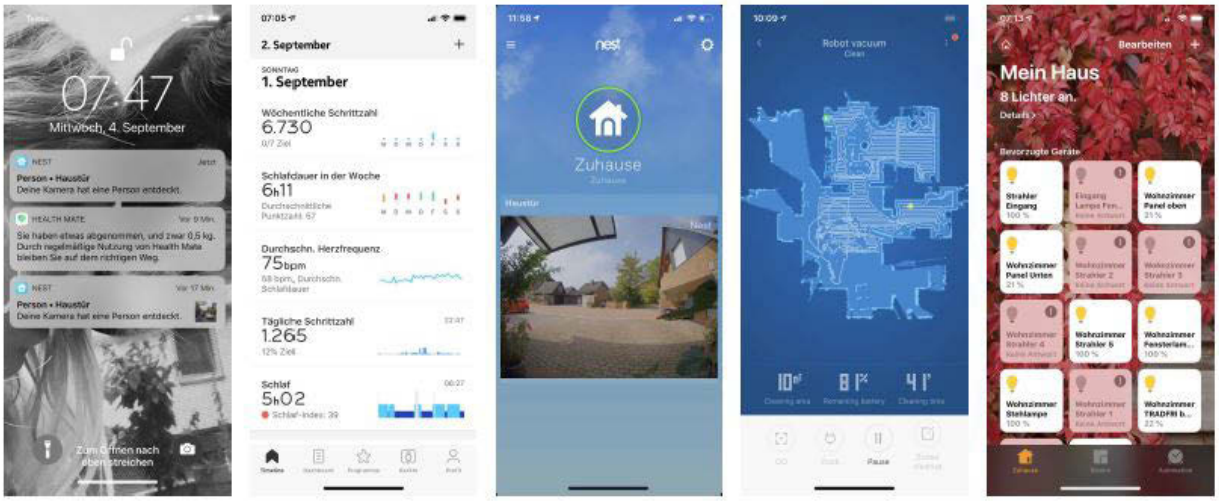
Es gilt das gesprochene Wort!

Meine sehr verehrten Damen und Herren,

der Vortrag „Gefahren erkennen, IT-Sicherheit schaffen“ des unabhängigen IT-Sicherheitsinstituts AV-TEST aus Magdeburg zeigt anhand von Mess- und Testdaten aktuelle Cyberbedrohungen auf, denen Anwender von internetbasierten Geräten tagtäglich ausgesetzt sind. Er erklärt kriminelle digitale Geschäftsmodelle für alle gängigen Geräte und Plattformen und dient der Lagebestimmung zur Einschätzung von Malware-Angriffen, Attacken auf Mobilgeräte und Smart Home-Infrastruktur und soll die Aufmerksamkeit der Nutzer zur Erreichung einer besseren Abwehr solcher Bedrohungen schärfen.

JETZT WIRD'S PERSÖNLICH:

Ich spreche über IT und IoT. Aber IT und IoT sprechen auch über mich...



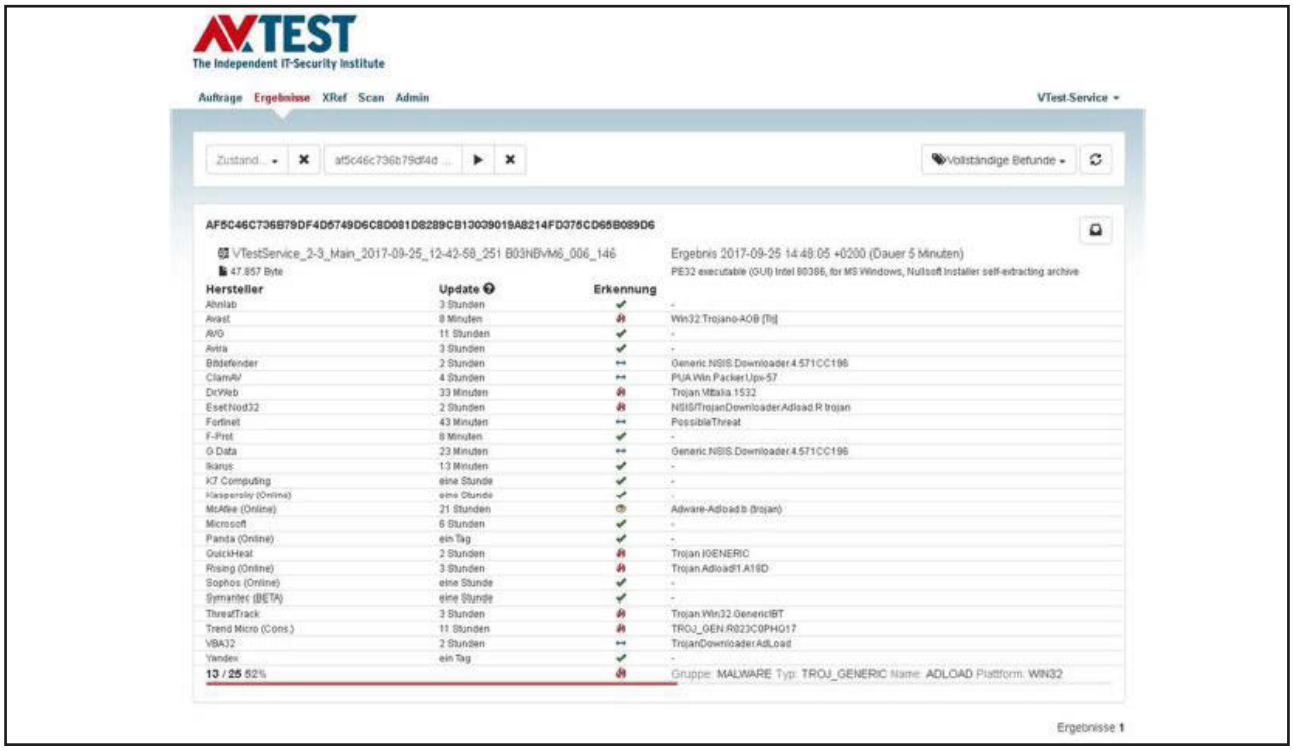
Das AV-TEST Institut:

Tests, Daten, Reports

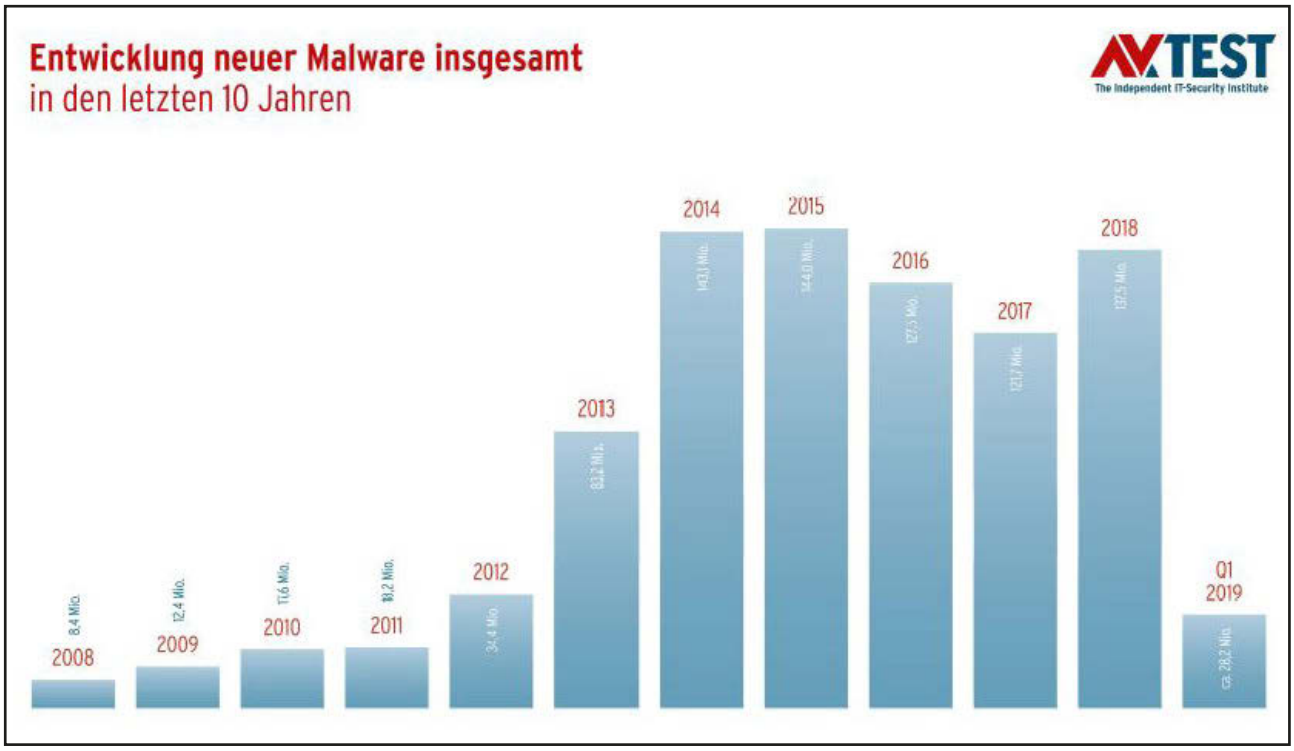
- MEHR ALS 30 IT-SPEZIALISTEN
- MEHR ALS 15 JAHRE EXPERTISE IM BEREICH ANTIVIREN-FORSCHUNG
- UNTERNEHMENSGRÜNDUNG 2004

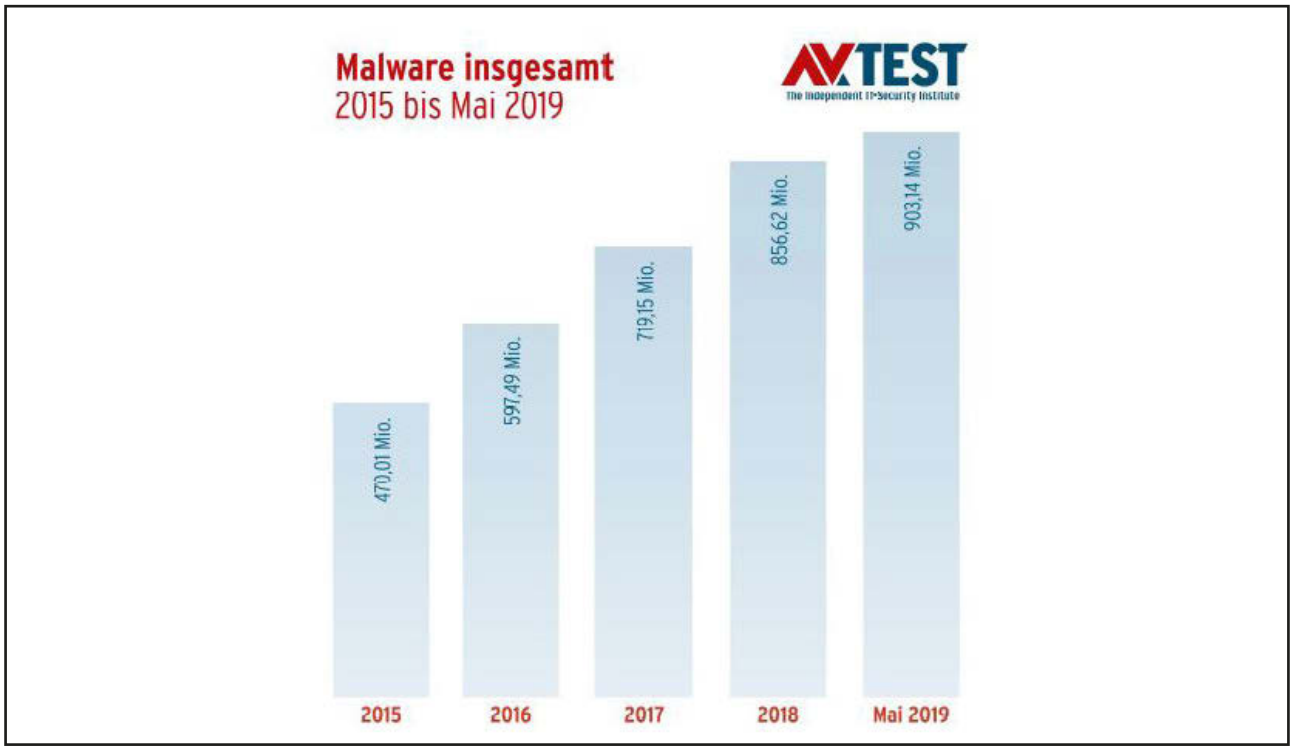
- EINE DER GRÖßTEN VIREN-DATENBANKEN DER WELT
- 500 CLIENT- UND SERVER-SYSTEME
- 2.500 TERABYTE TESTDATEN
- MEHR ALS 5.000 EINZEL- UND VERGLEICHSTESTS PRO JAHR

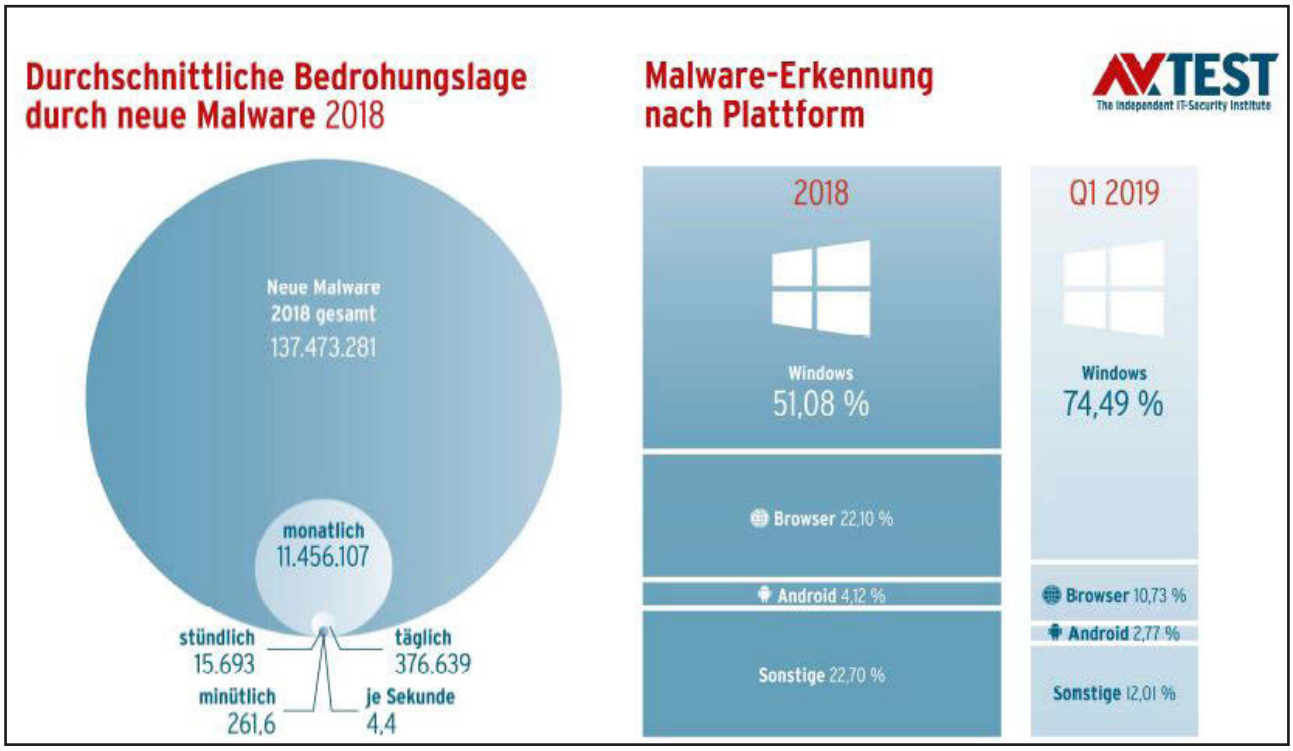
- ANALYSE, TESTING, DEVELOPMENT, CONSULTING & SERVICES FÜR AV-HERSTELLER, FACHMAGAZINE, BEHÖRDEN UND UNTERNEHMEN

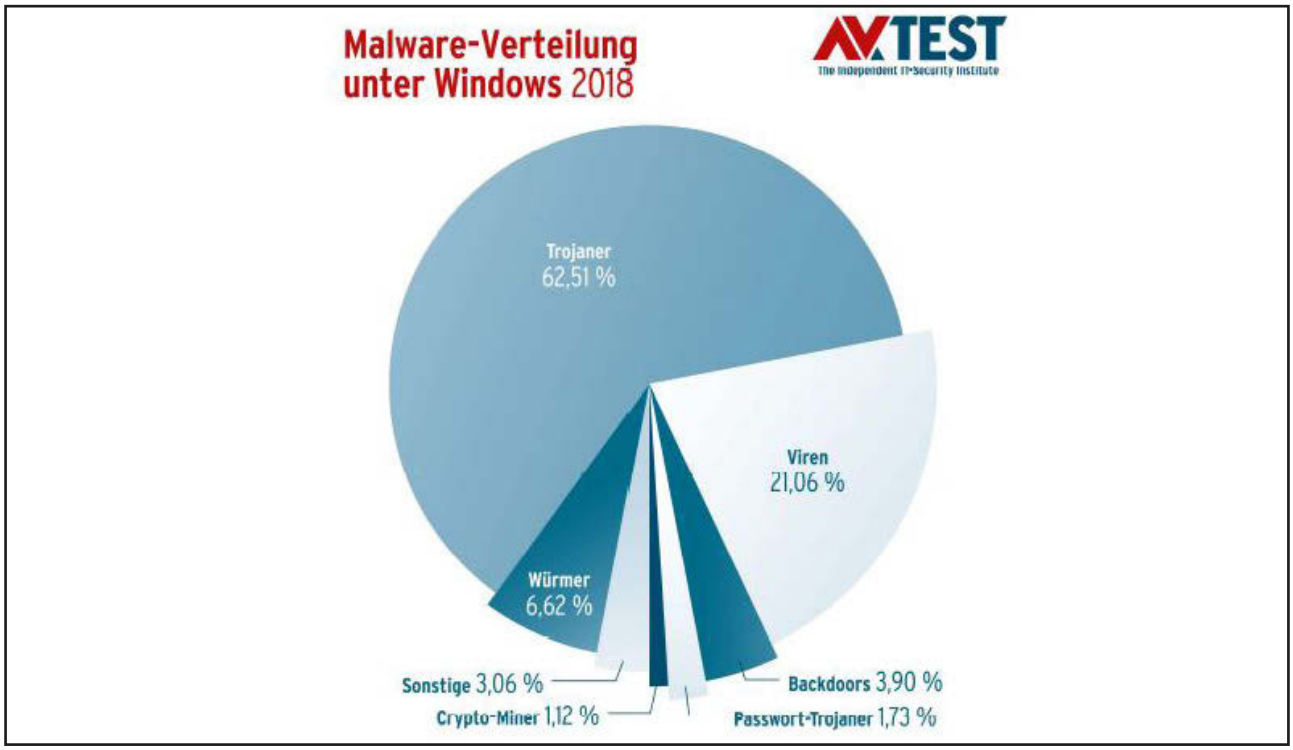

AV-TEST
The Independent IT-Security Institute
Aufträge Ergebnisse XRef Scan Admin
VTest-Service
Vollständige Befunde
AF5C46C736B79DF4D6749D6C8D081D8289CB1303901A8214FD375CD65B089D6
VTestService_2-3_Main_2017-09-25_12-42-58_251 B03NBVM6_006_146
47.857 Byte
Ergebnis 2017-09-25 14:48:05 +0200 (Dauer 5 Minuten)
PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Hersteller Update Erkennung
Ahnlab 3 Stunden -
Avast 8 Minuten Win32:Trojano-AOB [Trj]
AVG 11 Stunden -
Avira 3 Stunden -
Bitdefender 2 Stunden Generic.NSIS.Downloader.4.571CC196
ClamAV 4 Stunden PUA.Win.Packer.Upx-57
DrWeb 33 Minuten Trojan.Vtbaka.1532
EsetNod32 2 Stunden NSIS/TrojanDownloader.Adload.R trojan
Fortinet 43 Minuten PossibleThreat
F-Prot 8 Minuten -
G Data 23 Minuten Generic.NSIS.Downloader.4.571CC196
Ikarus 13 Minuten -
K7 Computing eine Stunde -
Kaspersky (Online) eine Stunde -
McAfee (Online) 21 Stunden Adware-Adload.b (trojan)
Microsoft 6 Stunden -
Panda (Online) ein Tag -
QuickHeal 2 Stunden Trojan.IGENERIC
Rising (Online) 3 Stunden Trojan.Adload!1.A18D
Sophos (Online) eine Stunde -
Symantec (BETA) eine Stunde -
ThreatTrack 3 Stunden Trojan.Win32.GenericIBT
Trend Micro (Cons.) 11 Stunden TROJ_GEN.R023C0PHQ17
VBA32 2 Stunden TrojanDownloader:AdLoad
Yandex ein Tag -
13 / 25 52%
Gruppe: MALWARE Typ: TROJ_GENERIC Name: ADLOAD Plattform: WIN32
Ergebnisse 1


AegisLab
AhnLab
Avira
Baidu
Bitdefender
Bornaria
BullGuard
Carbon Black.
Check Point
COMODO
CYLANCE
Dr. Web
DU Group
EMSISOFT
ESET
F-Secure
G-Protector
GFI
HAURI
IKARUS
intego
invincea
Jarviz
Juniper
K7 COMPUTING
KASPERSKY
KSmobile
Lookout
Malwarebytes
McAfee
Microsoft
eScan
NORMAN
NQ mobile
NSHC
panda
PCKEEPER
PC Pitstop
PLAY CASTLE
PSafe
Quick Heal
secucloud
SentinelOne
SEQRITE
SOPHOS
SUVsoft
Symantec
ThreatTrack
total defense
TREND MICRO
TrustGo
Trustlook
VIPRE
WEBROOT
White Gate
Zoner AntiVirus
AV-TEST
The Independent IT-Security Institute

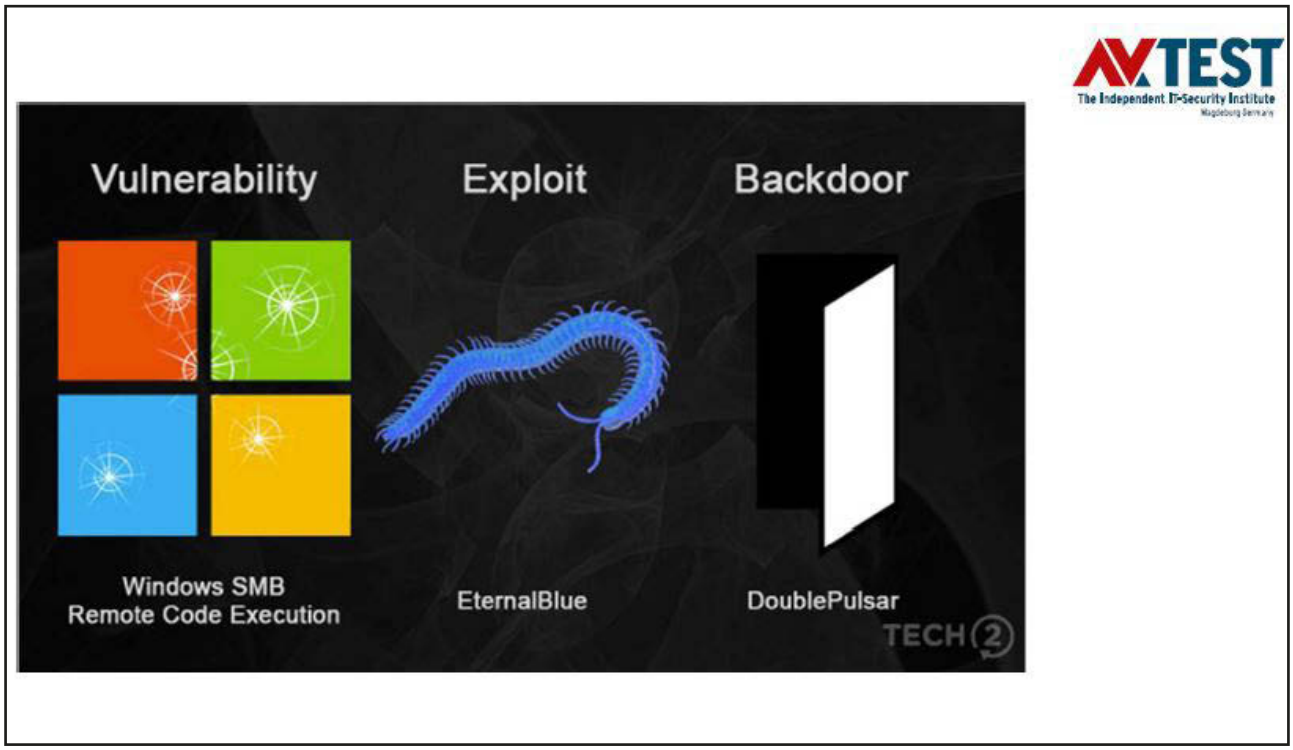

Entwicklung neuer Malware insgesamt
in den letzten 10 Jahren
AV-TEST
The Independent IT-Security Institute
2008
8,4 Mio.
2009
12,4 Mio.
2010
11,6 Mio.
2011
18,2 Mio.
2012
34,4 Mio.
2013
83,2 Mio.
2014
143,1 Mio.
2015
144,0 Mio.
2016
127,3 Mio.
2017
121,7 Mio.
2018
137,5 Mio.
Q1
2019
ca. 28,2 Mio.


Malware insgesamt
2015 bis Mai 2019
AV-TEST
The Independent IT-Security Institute
470,01 Mio.
2015
597,49 Mio.
2016
719,15 Mio.
2017
856,62 Mio.
2018
903,14 Mio.
Mai 2019

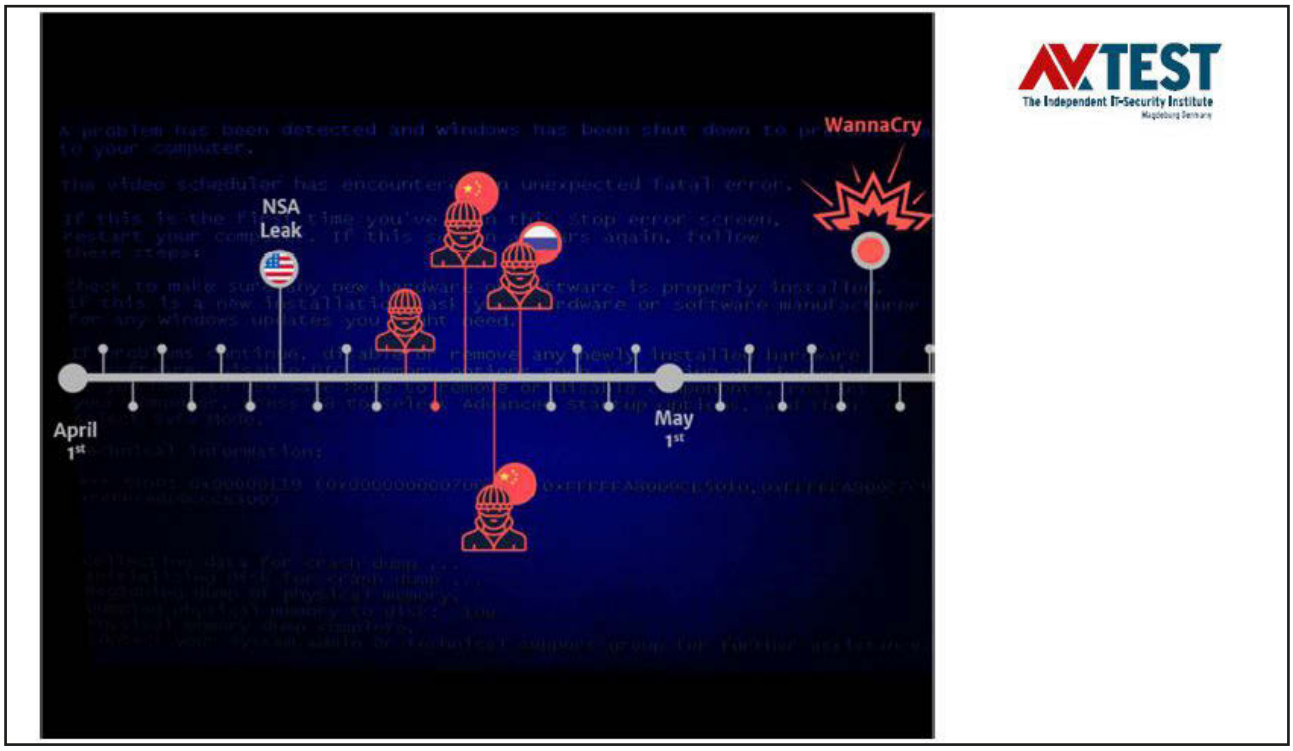

Durchschnittliche Bedrohungslage durch neue Malware 2018
Neue Malware 2018 gesamt 137.473.281
monatlich 11.456.107
stündlich 15.693
täglich 376.639
minütlich 261,6
je Sekunde 4,4
Malware-Erkennung nach Plattform
AV-TEST The Independent IT-Security Institute
2018
Windows 51,08 %
Browser 22,10 %
Android 4,12 %
Sonstige 22,70 %
Q1 2019
Windows 74,49 %
Browser 10,73 %
Android 2,77 %
Sonstige 12,01 %


Malware-Verteilung unter Windows 2018
AV-TEST The Independent IT-Security Institute
Trojaner 62,51 %
Viren 21,06 %
Würmer 6,62 %
Sonstige 3,06 %
Crypto-Miner 1,12 %
Backdoors 3,90 %
Passwort-Trojaner 1,73 %


AV-TEST
The Independent IT-Security Institute
Windows: Entwicklung neuer Exploits
2018 + Q1 2019
12.614
10.410
5.584
Januar 2018
Oktober 2018
März 2019


AV-TEST
The Independent IT-Security Institute
Vulnerability
Exploit
Backdoor
Windows SMB
Remote Code Execution
EternalBlue
DoublePulsar
TECH 2


AV-TEST
The Independent IT-Security Institute
patch me if you can


AV-TEST
The Independent IT-Security Institute
WannaCry
NSA
Leak
April
1st
May
1st

SPIEGEL ONLINE

Krankenhaus in Not

Computervirus legt bayerische Klinik lahm

Seit Tagen sind im Klinikum Fürstenfeldbruck Hunderte Computer unbenutzbar. Ein Computervirus, der eigentlich andere Ziele sucht, hatte die Systeme befallen.

Mediziner vor Computer (Symbolbild)

Ein Computervirus hat im Klinikum Fürstenfeldbruck offenbar beträchtlichen Schaden angerichtet. Die Zentralstelle Cybercrime Bayern hat Ermittlungen dem Vorfall aufgenommen, der die IT-Systeme des Krankenhauses tagelang lahmlegte.

AV-TEST The Independent IT-Security Institute

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

Lee Mathews

In June, the NotPetya ransomware hit companies in the U.S. and throughout Europe. One of those hardest hit was Copenhagen-based shipping giant A.P. Moller-Maersk, which moves about one-fifth of the world's freight. Operations at Maersk terminals in four different countries were impacted, causing delays and disruption that lasted weeks.

AV-TEST The Independent IT-Security Institute

Microsoft-Sicherheitsbulletin MS17-010 – Kritisch

Sicherheitsupdate für Microsoft Windows SMB-Server (4013389)

Veröffentlicht: 14. März 2017

Version: 1.0

Kurzzusammenfassung

Dieses Sicherheitsupdate behebt Sicherheitsanfälligkeiten in Microsoft Windows. Die schwerwiegendste dieser Sicherheitsanfälligkeiten kann Remotecode ausführung ermöglichen, wenn ein Angreifer eine Reihe speziell gestalteter Nachrichten an einen betroffenen Windows SMBv1-Server sendet.

Dieses Sicherheitsupdate wird für alle unterstützten Versionen von Microsoft Windows als „Kritisch" eingestuft. Weitere Informationen finden Sie unter **Betroffene Software und Bewertungen des Schweregrads der Sicherheitsanfälligkeit**.

Das Sicherheitsupdate behebt die Sicherheitsanfälligkeiten, indem korrigiert wird, wie SMBv1 speziell gestaltete Anforderungen verarbeitet.

Weitere Informationen zu den Sicherheitsanfälligkeiten finden Sie im Abschnitt **Informationen zu Sicherheitsanfälligkeiten**.

Weitere Informationen zu diesem Update finden Sie im Microsoft Knowledge Base-Artikel 4013389.

Auf dieser Seite

Betroffene Software und Bewertungen des Schweregrads der Sicherheitsanfälligkeit

Betreff: Stefan Friedrich - Bewerbung
Datum: Mon, 05 Dec 2016 08:26:57 +0000
Von: Stefan Friedrich <s.friedrich@t-online.de> Antwort an: Stefan Friedrich <s.friedrich@t-online.de>
An: [redacted]

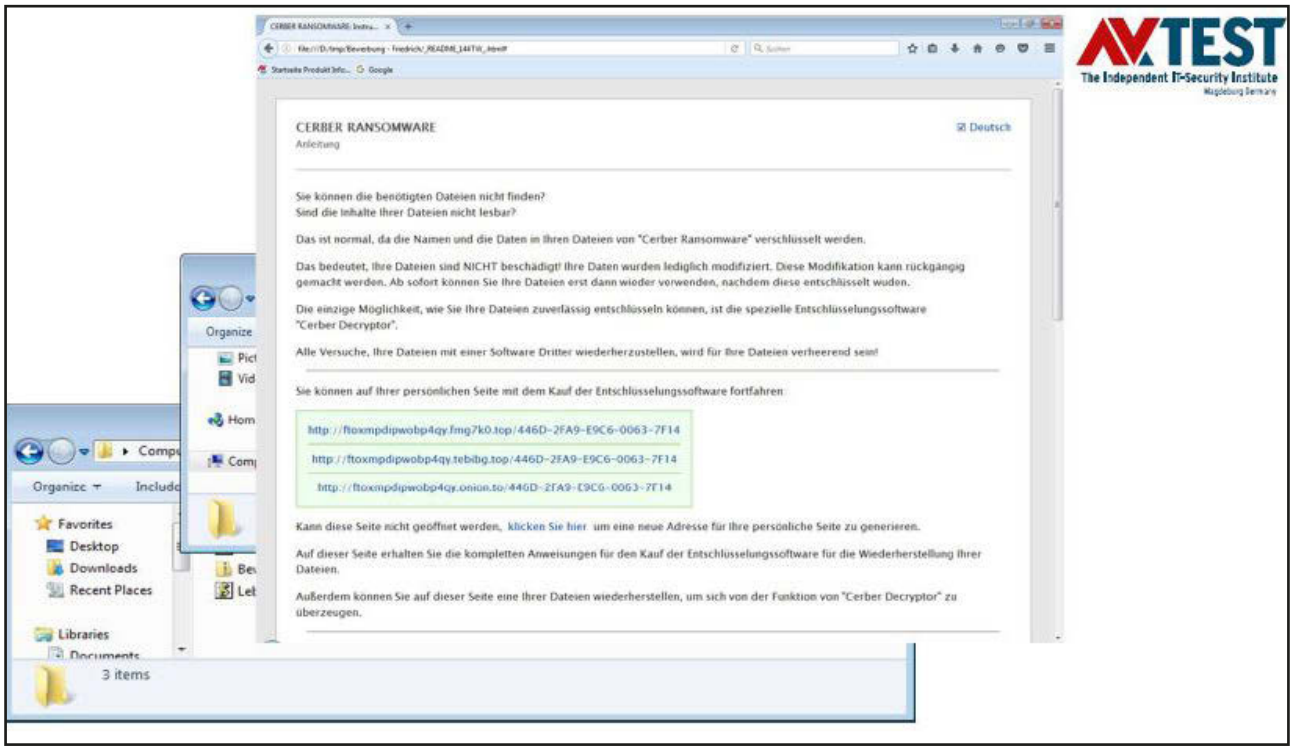
Sehr geehrte Damen und Herren,

anbei finden Sie meine Bewerbung für Ihre ausgeschriebene Position. Die Stelle entspricht genau meinen Vorstellungen und reizt mich sehr. Da mein Profil und meine bisherigen Erfahrungen gut zu Ihren Anforderungen passen, bin ich davon überzeugt, einen echten Mehrwert leisten zu können. Und das möchte ich!

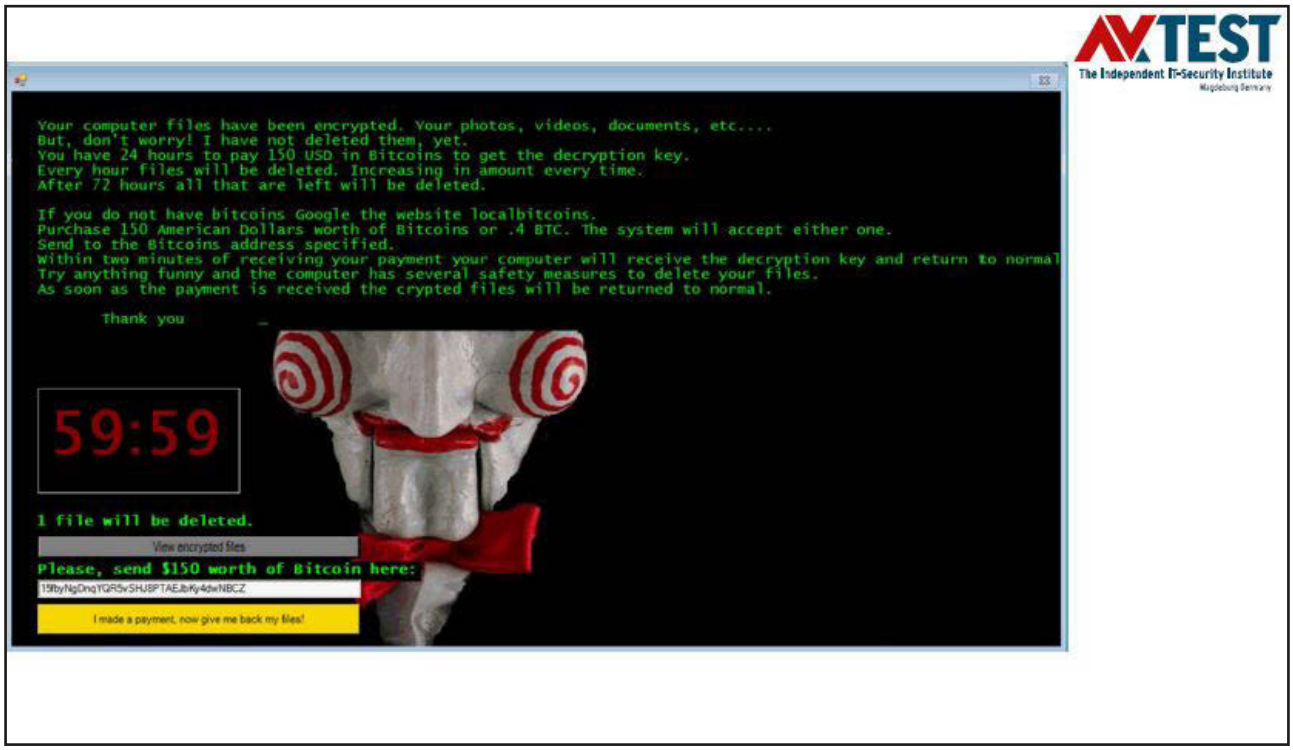
Ich freue mich, wenn Sie meine Bewerbungsunterlagen im Anhang prüfen und ich mich Ihnen noch einmal persönlich vorstellen kann.

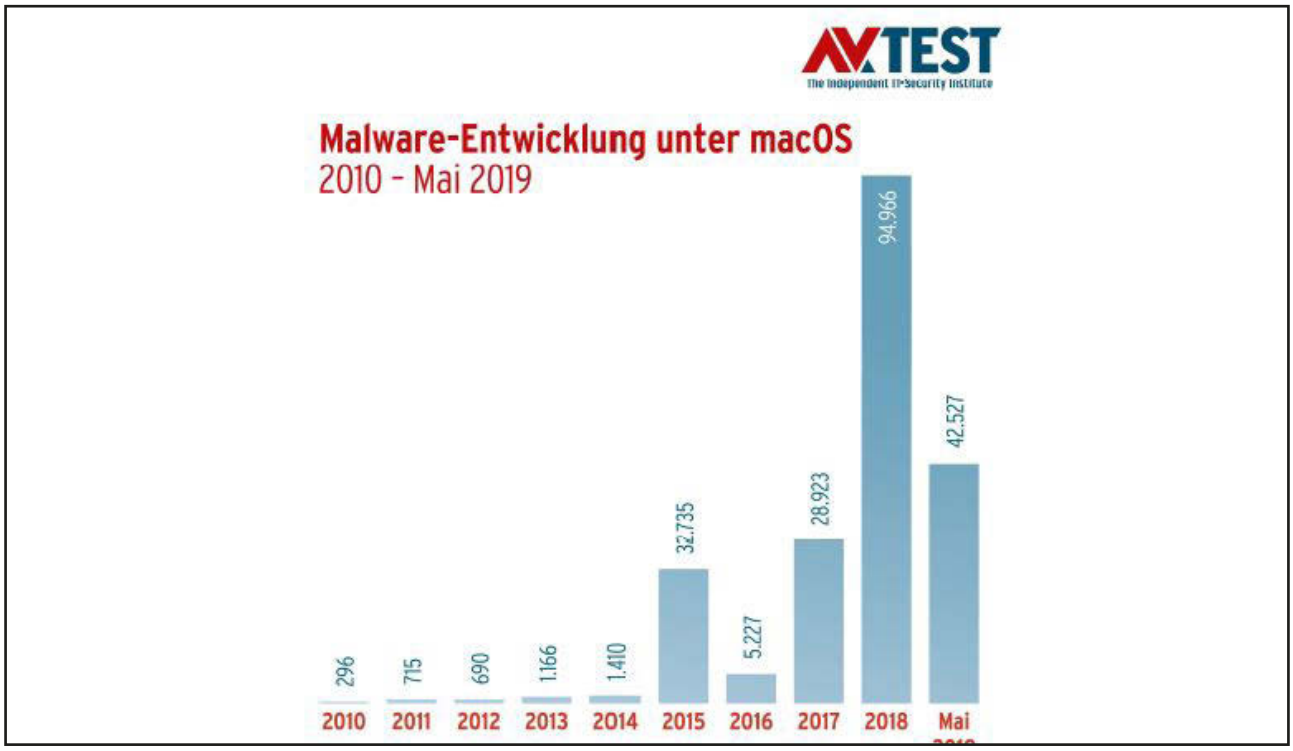
Mit besten Grüßen,

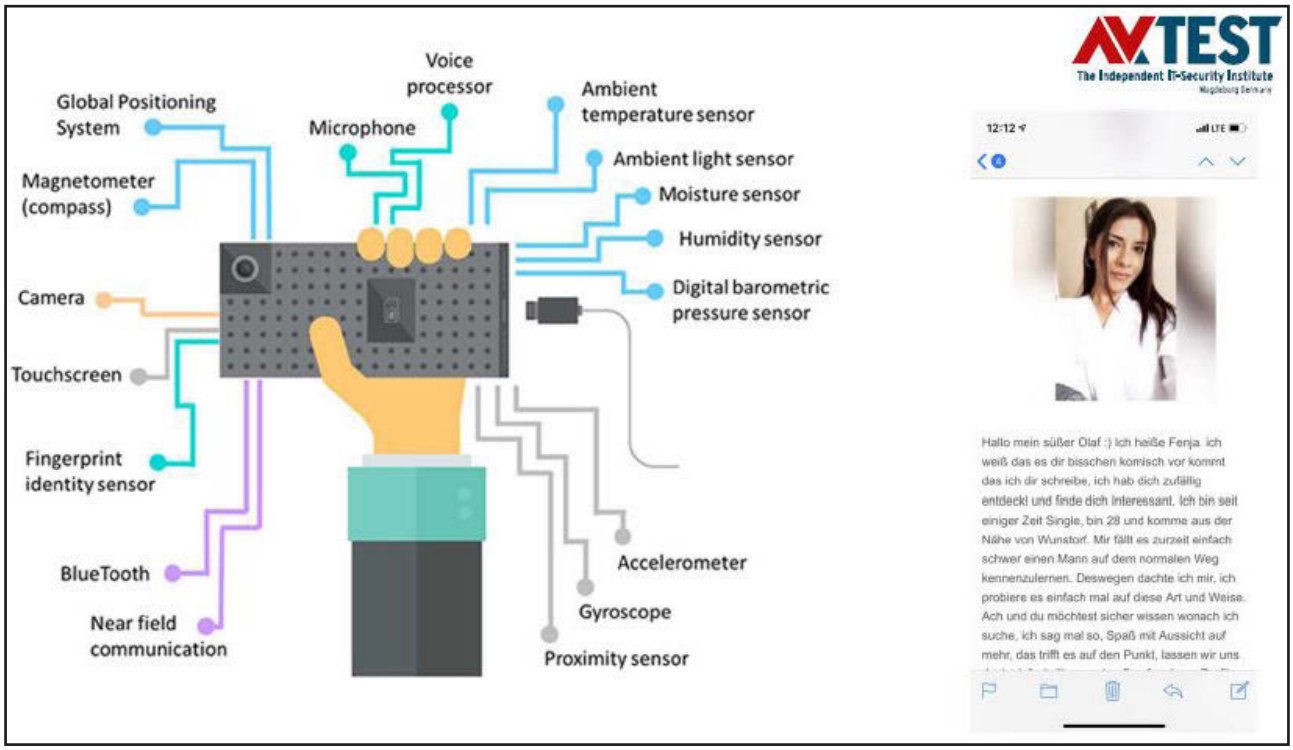
Stefan Friedrich

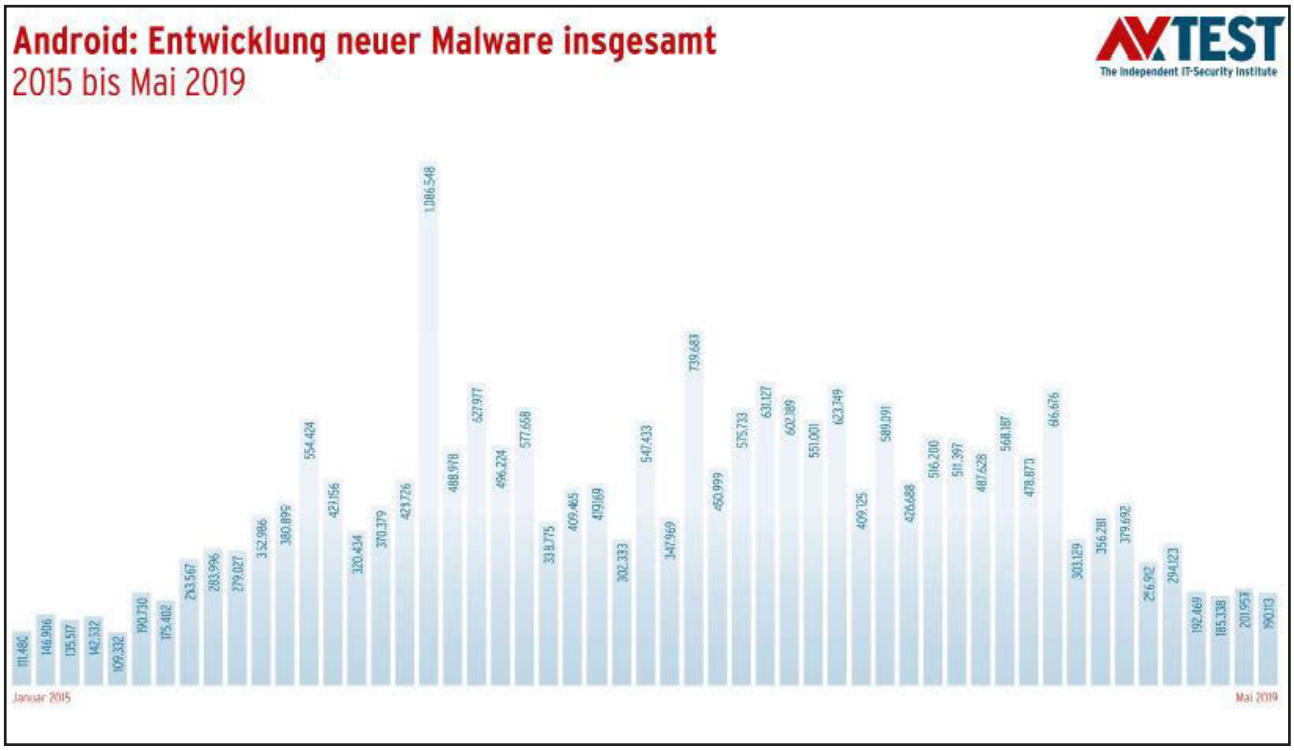


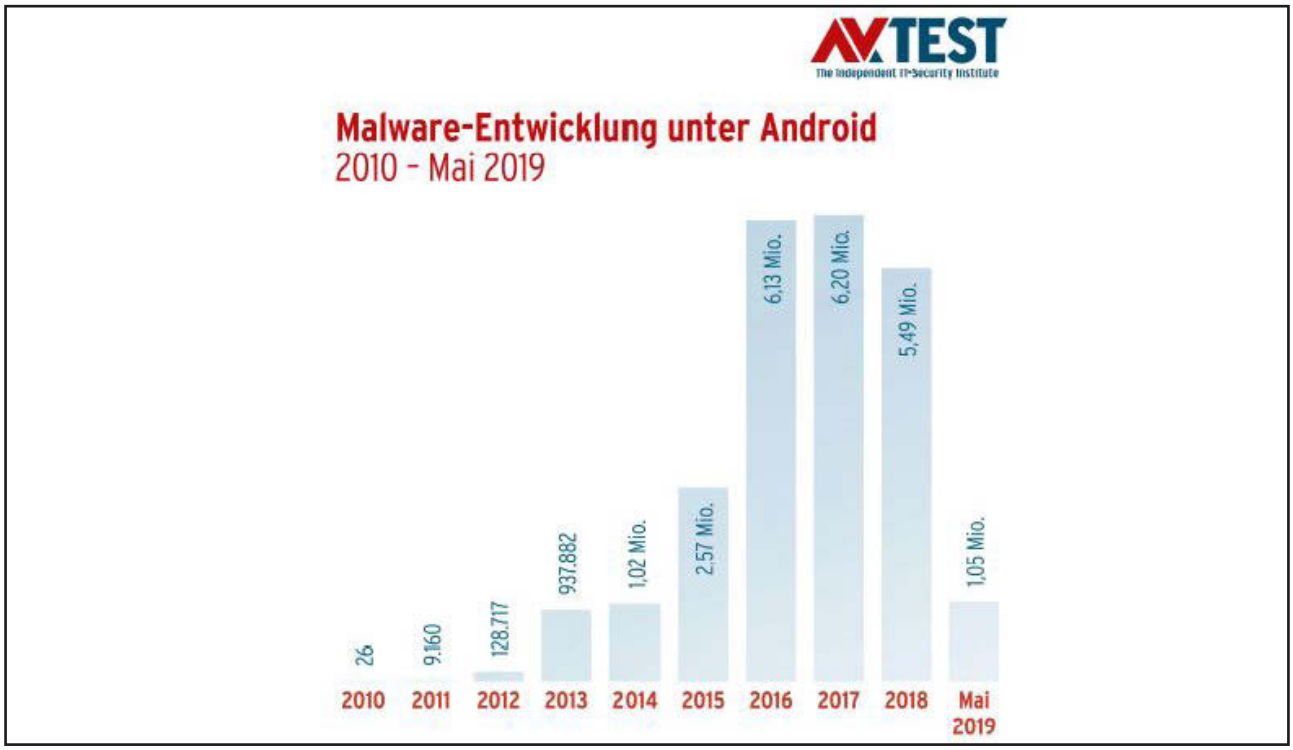

THE DARK ENCRYPTOR
All your files have been encrypted
by THE DARK ENCRYPTOR using a military
grade encryption algorithm.
But dont worry ! You can get them
back, you just need to pay 100 USD
in bitcoin. For more informations,
please read the text document placed
on your Desktop.
Have a nice day !
WARNING: The price will rise to
350 USD if you don't pay
in the next 5 days.
AV-TEST
The Independent IT-Security Institute

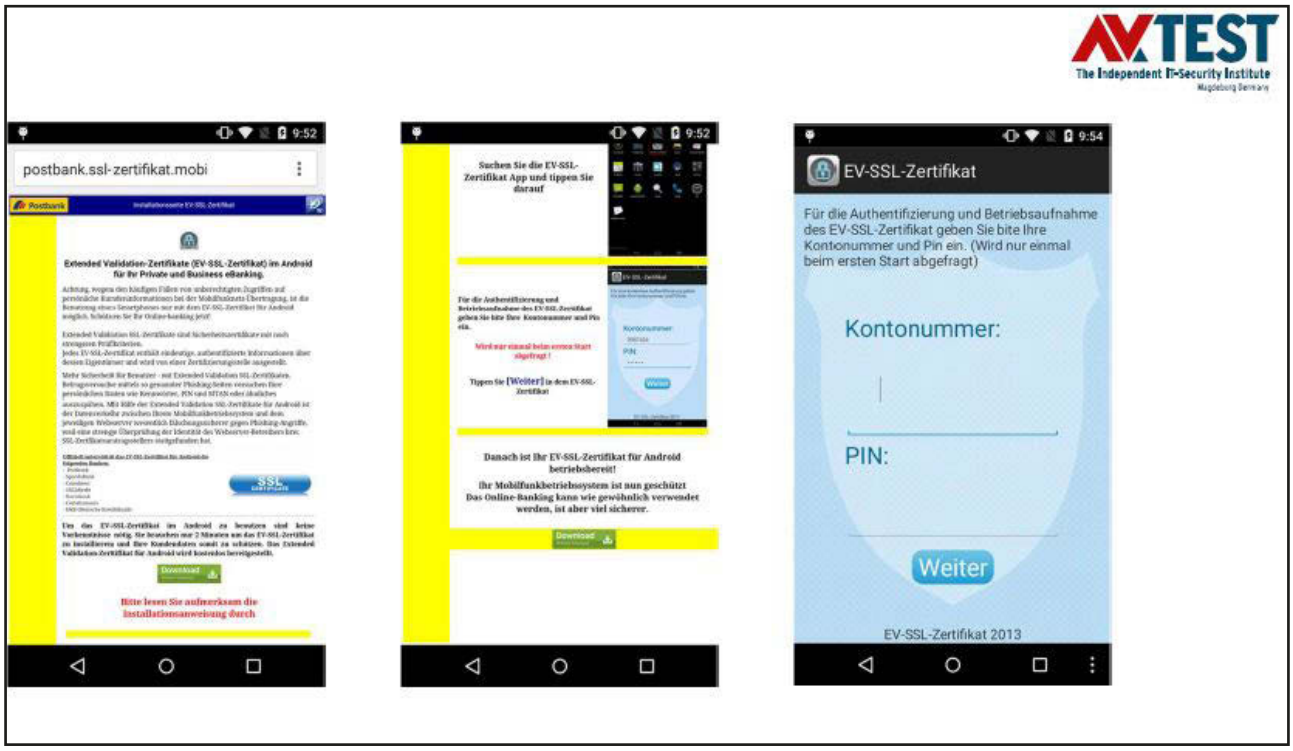

Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.
If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypted files will be returned to normal.
Thank you
59:59
1 file will be deleted.
View encrypted files
Please, send $150 worth of Bitcoin here:
15fbyNgDnqYQR5vSHJSPTAEJbKy4dwNBCZ
I made a payment, now give me back my files!
AV-TEST
The Independent IT-Security Institute

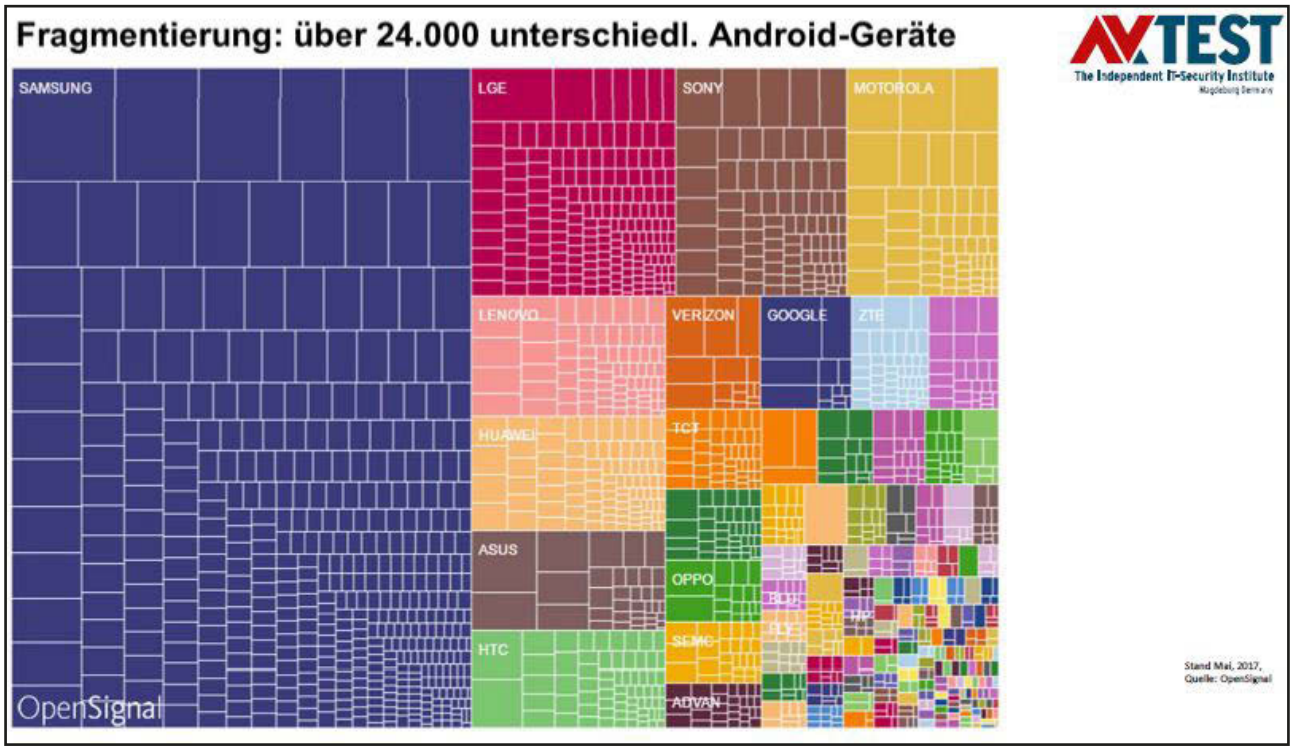

AV-TEST
The Independent IT-Security Institute
Malware-Entwicklung unter macOS
2010 - Mai 2019
296
715
690
1.166
1.410
32.735
5.227
28.923
94.966
42.527
2010
2011
2012
2013
2014
2015
2016
2017
2018
Mai


Global Positioning System
Magnetometer (compass)
Camera
Touchscreen
Fingerprint identity sensor
BlueTooth
Near field communication
Voice processor
Microphone
Ambient temperature sensor
Ambient light sensor
Moisture sensor
Humidity sensor
Digital barometric pressure sensor
Accelerometer
Gyroscope
Proximity sensor
AV-TEST
The Independent IT-Security Institute
Hallo mein süßer Olaf :) Ich heiße Fenja. ich weiß das es dir bisschen komisch vor kommt das ich dir schreibe, ich hab dich zufällig entdeckt und finde dich interessant. Ich bin seit einiger Zeit Single, bin 28 und komme aus der Nähe von Wunstorf. Mir fällt es zurzeit einfach schwer einen Mann auf dem normalen Weg kennenzulernen. Deswegen dachte ich mir, ich probiere es einfach mal auf diese Art und Weise. Ach und du möchtest sicher wissen wonach ich suche, ich sag mal so, Spaß mit Aussicht auf mehr, das trifft es auf den Punkt, lassen wir uns


Android: Entwicklung neuer Malware insgesamt
2015 bis Mai 2019
AV-TEST
The Independent IT-Security Institute
111.486
146.906
135.517
142.532
109.332
190.730
175.402
263.567
283.996
279.027
352.986
380.895
554.424
421.156
320.434
370.379
423.726
1.086.548
488.978
627.977
496.224
577.658
318.775
409.465
419.169
302.333
547.433
347.969
739.683
450.999
575.733
631.127
602.389
551.001
623.749
409.125
589.091
426.688
516.200
511.397
487.628
568.187
478.873
696.676
303.129
356.281
379.692
276.912
294.123
192.469
185.338
201.958
190.113
Januar 2015
Mai 2019


AV-TEST
The Independent IT-Security Institute
Malware-Entwicklung unter Android
2010 - Mai 2019
26
9.160
128.717
937.882
1,02 Mio.
2,57 Mio.
6,13 Mio.
6,20 Mio.
5,49 Mio.
1,05 Mio.
2010
2011
2012
2013
2014
2015
2016
2017
2018
Mai 2019


AV-TEST
The Independent IT-Security Institute
Magdeburg Germany
postbank.ssl-zertifikat.mobi
Extended Validation-Zertifikate (EV-SSL-Zertifikat) im Android für Ihr Private und Business eBanking.
Download
Bitte lesen Sie aufmerksam die Installationsanweisung durch
Suchen Sie die EV-SSL-Zertifikat App und tippen Sie darauf
Danach ist Ihr EV-SSL-Zertifikat für Android betriebsbereit!
Ihr Mobilfunkbetriebssystem ist nun geschützt
Das Online-Banking kann wie gewöhnlich verwendet werden, ist aber viel sicherer.
EV-SSL-Zertifikat
Für die Authentifizierung und Betriebsaufnahme des EV-SSL-Zertifikat geben Sie bitte Ihre Kontonummer und Pin ein. (Wird nur einmal beim ersten Start abgefragt)
Kontonummer:
PIN:
Weiter
EV-SSL-Zertifikat 2013


Fragmentierung: über 24.000 unterschiedl. Android-Geräte
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany
SAMSUNG
LGE
SONY
MOTOROLA
LENOVO
VERIZON
GOOGLE
ZTE
HUAWEI
TCT
ASUS
OPPO
HTC
SEMC
ADVAN
OpenSignal
Stand Mai, 2017,
Quelle: OpenSignal

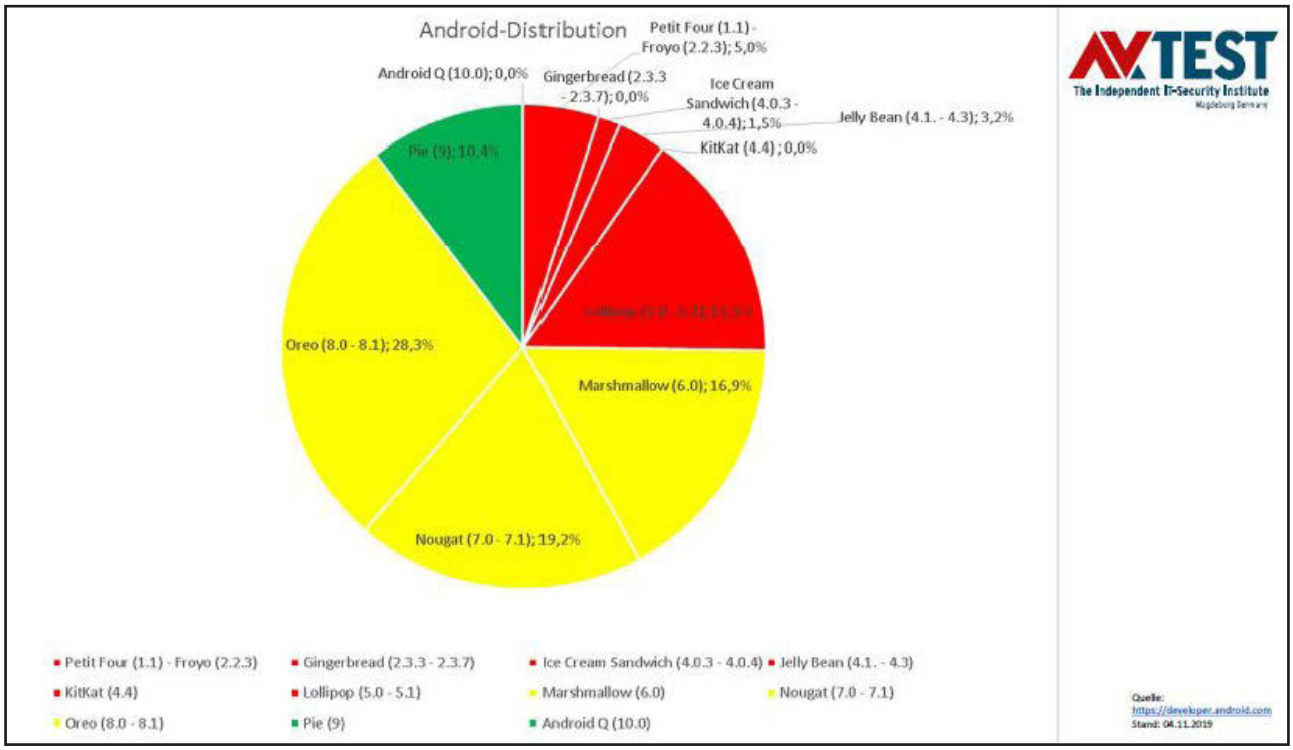
Update: Massenhaft Geräte nicht auf letztem Stand

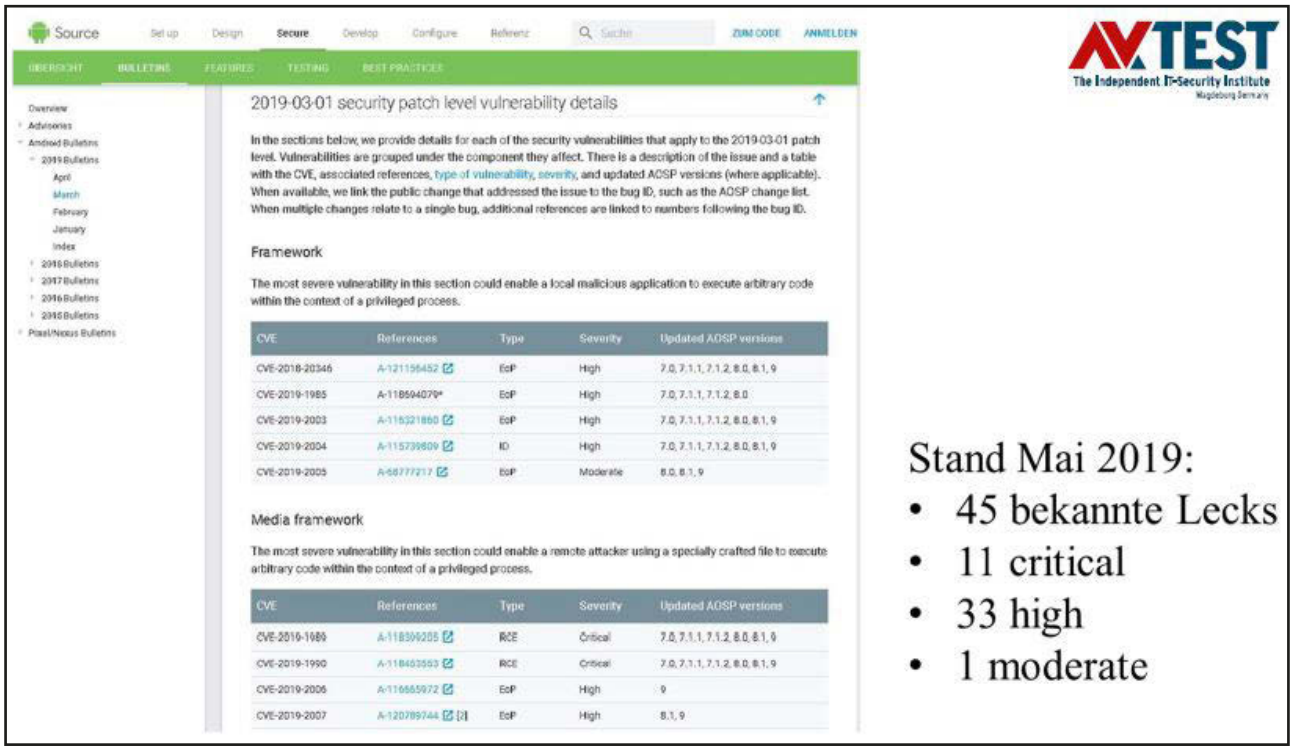
AV-TEST The Independent IT-Security Institute Magdeburg Germany

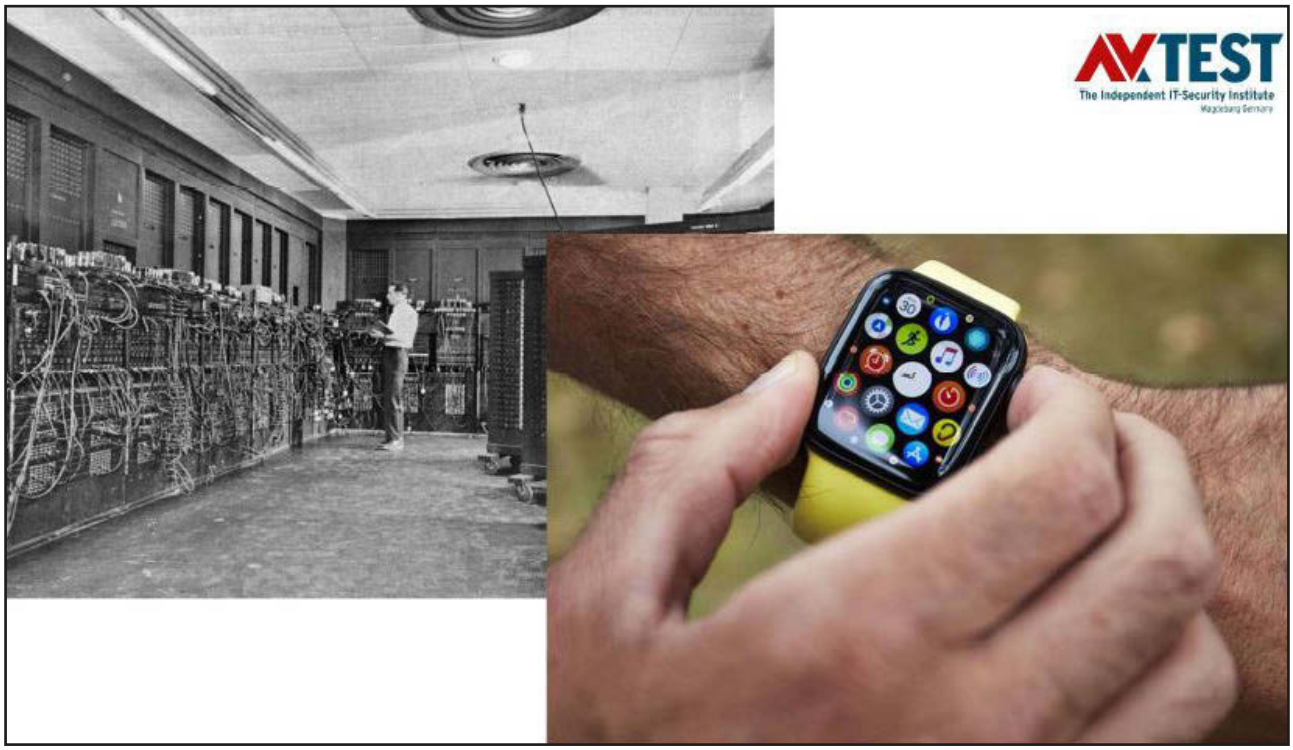
Code name	Version number	Linux kernel version[1]	Initial release date	API level	Ref
(No codename)	1.0	?	September 23, 2008	1	[2]
Petit Four	1.1	2.6	February 9, 2009	2	[2]
Cupcake	1.5	2.6.27	April 27, 2009	3	
Donut	1.6	2.6.29	September 15, 2009	4	[3]
Eclair	2.0 – 2.1	2.6.29	October 26, 2009	5 – 7	[4]
Froyo	2.2 – 2.2.3	2.6.32	May 20, 2010	8	[5]
Gingerbread	2.3 – 2.3.7	2.6.35	December 6, 2010	9 – 10	[6]
Honeycomb	3.0 – 3.2.6	2.6.36	February 22, 2011	11 – 13	[7]
Ice Cream Sandwich	4.0 – 4.0.4	3.0.1	October 18, 2011	14 – 15	[8]
Jelly Bean	4.1 – 4.3.1	3.0.31 to 3.4.39	July 9, 2012	16 – 18	[9]
KitKat	4.4 – 4.4.4	3.10	October 31, 2013	19 – 20	[10]
Lollipop	5.0 – 5.1.1	3.16	November 12, 2014	21 – 22	[11]
Marshmallow	6.0 – 6.0.1	3.18	October 5, 2015	23	[12]
Nougat	7.0 – 7.1.2	4.4	August 22, 2016	24 – 25	[13]
Oreo	8.0 – 8.1	4.10	August 21, 2017	26 – 27	[14]
Pie	**9.0**	4.4.107, 4.9.84, and 4.14.42	August 6, 2018	28	[15]
Android Q	10.0			29	

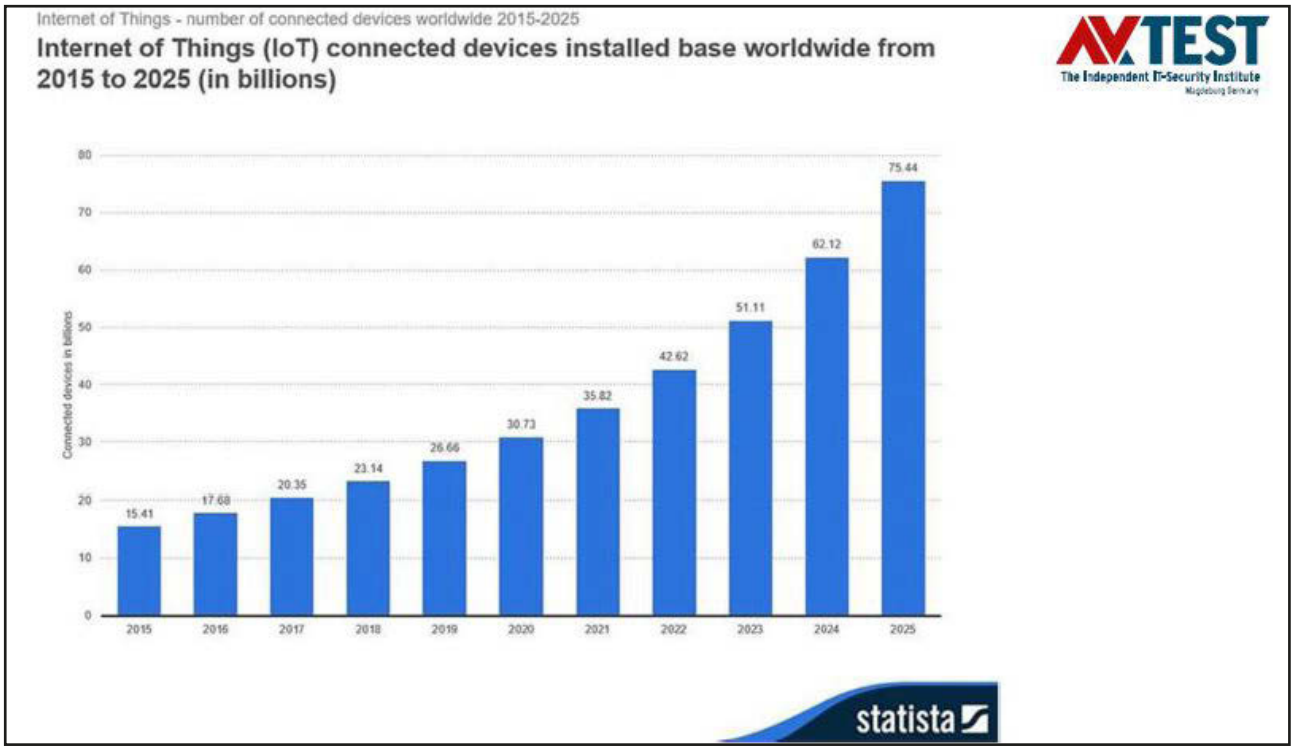
Legend: Old version | Older version, still supported | **Latest version** | Latest preview version

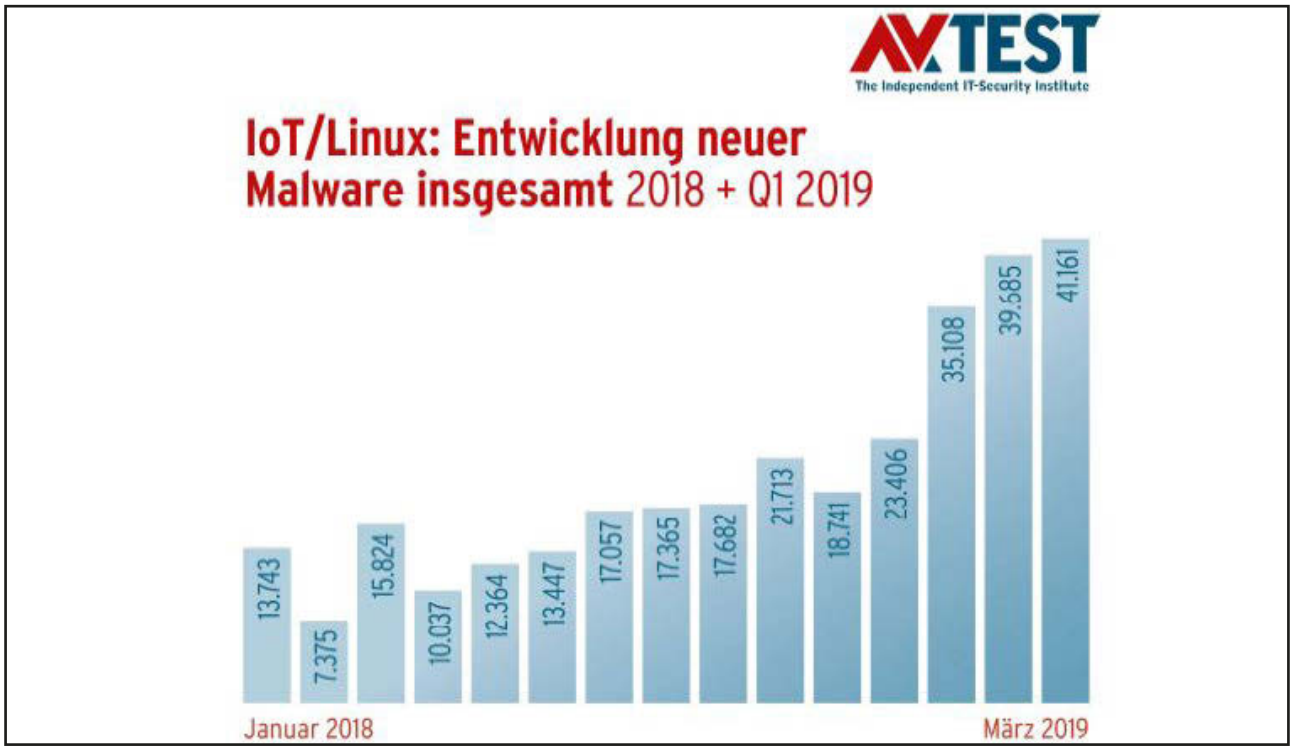
Stand Q3 2018, Quelle: Google

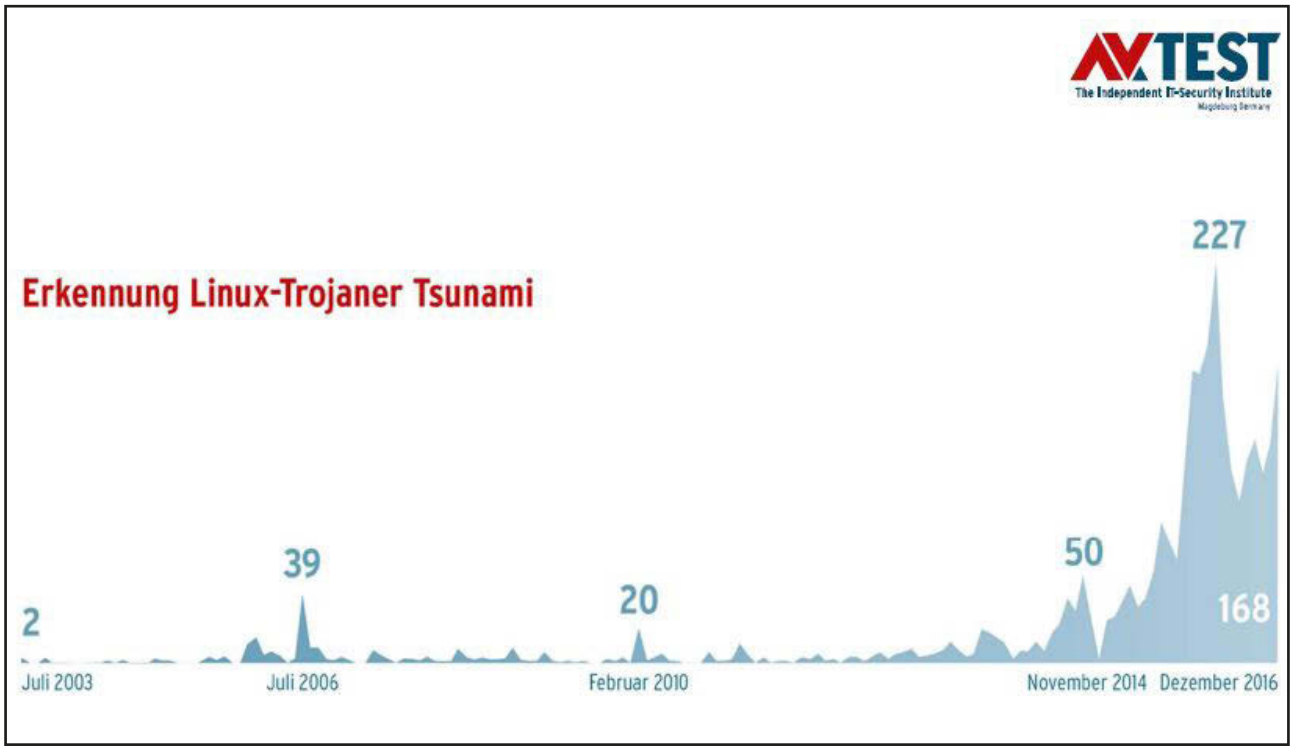


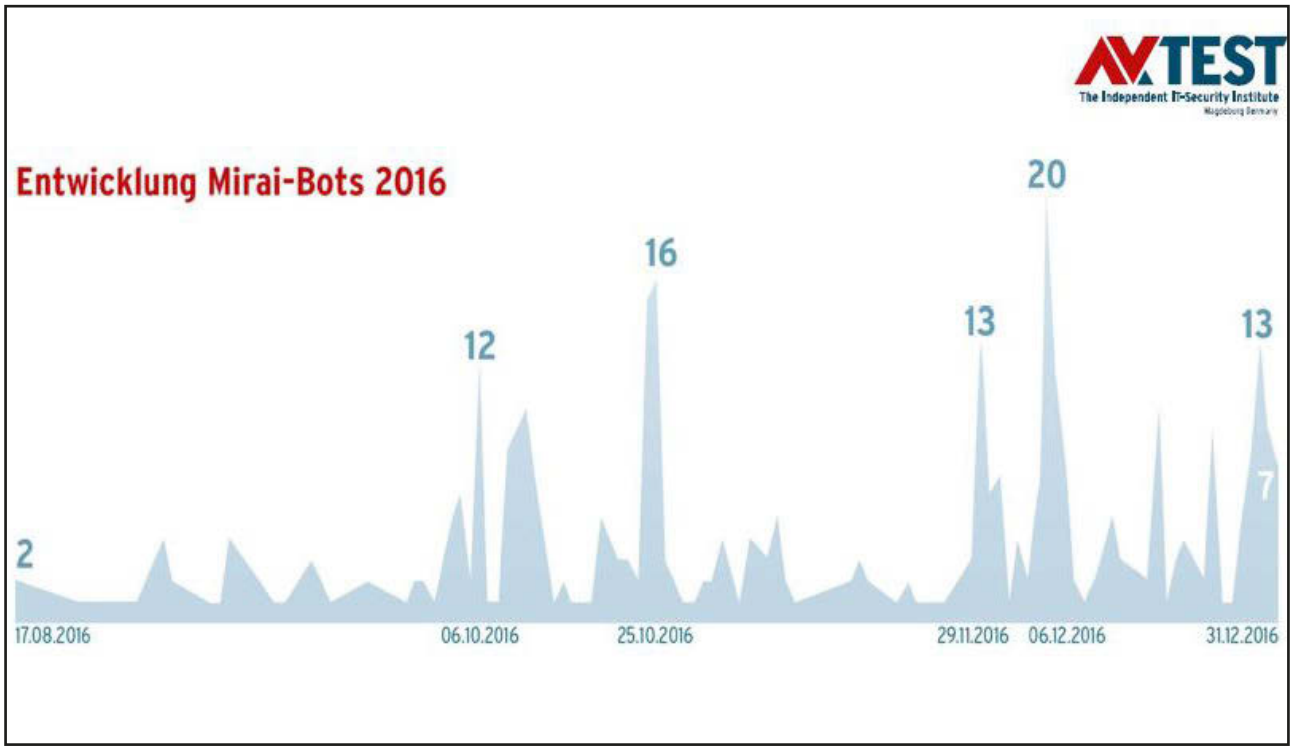

Source
Set up
Design
Secure
Develop
Configure
Referenz
ZUM CODE
ANMELDEN
ÜBERSICHT
BULLETINS
FEATURES
TESTING
BEST PRACTICES
Overview
Advisories
Android Bulletins
2019 Bulletins
April
March
February
January
Index
2018 Bulletins
2017 Bulletins
2016 Bulletins
2015 Bulletins
Pixel/Nexus Bulletins
2019-03-01 security patch level vulnerability details
In the sections below, we provide details for each of the security vulnerabilities that apply to the 2019-03-01 patch level. Vulnerabilities are grouped under the component they affect. There is a description of the issue and a table with the CVE, associated references, type of vulnerability, severity, and updated AOSP versions (where applicable). When available, we link the public change that addressed the issue to the bug ID, such as the AOSP change list. When multiple changes relate to a single bug, additional references are linked to numbers following the bug ID.
Framework
The most severe vulnerability in this section could enable a local malicious application to execute arbitrary code within the context of a privileged process.
CVE
References
Type
Severity
Updated AOSP versions
CVE-2018-20346
A-121156452
EoP
High
7.0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-1985
A-118594079*
EoP
High
7.0, 7.1.1, 7.1.2, 8.0
CVE-2019-2003
A-116321860
EoP
High
7.0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2004
A-115739809
ID
High
7.0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2005
A-68777217
EoP
Moderate
8.0, 8.1, 9
Media framework
The most severe vulnerability in this section could enable a remote attacker using a specially crafted file to execute arbitrary code within the context of a privileged process.
CVE
References
Type
Severity
Updated AOSP versions
CVE-2019-1989
A-118399285
RCE
Critical
7.0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-1990
A-118403553
RCE
Critical
7.0, 7.1.1, 7.1.2, 8.0, 8.1, 9
CVE-2019-2006
A-116655972
EoP
High
9
CVE-2019-2007
A-120789744
EoP
High
8.1, 9
AV TEST
The Independent IT-Security Institute
Magdeburg Germany
Stand Mai 2019:
• 45 bekannte Lecks
• 11 critical
• 33 high
• 1 moderate

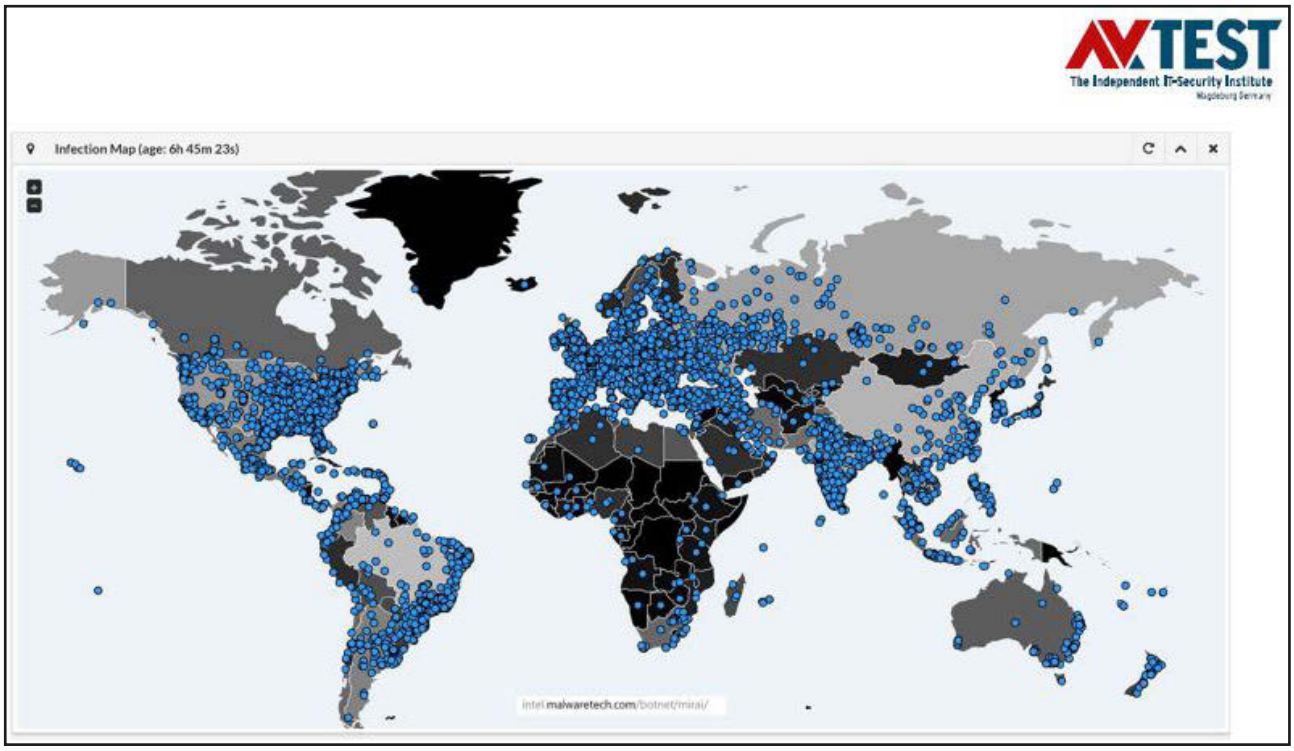

AV TEST
The Independent IT-Security Institute
Magdeburg Germany

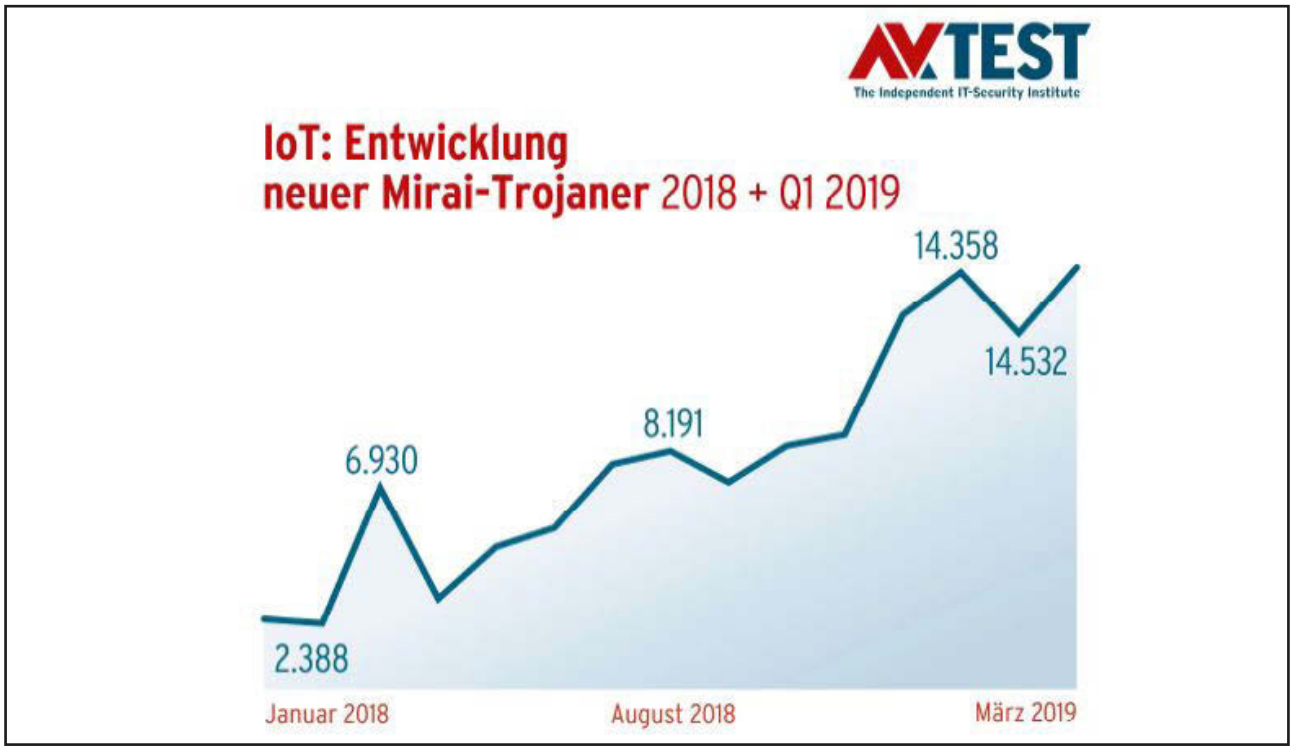

Internet of Things - number of connected devices worldwide 2015-2025
Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)
AV-TEST
The Independent IT-Security Institute
Connected devices in billions
80
70
60
50
40
30
20
10
0
15.41
17.68
20.35
23.14
26.66
30.73
35.82
42.62
51.11
62.12
75.44
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
statista


AV-TEST
The Independent IT-Security Institute
IoT/Linux: Entwicklung neuer Malware insgesamt 2018 + Q1 2019
13.743
7.375
15.824
10.037
12.364
13.447
17.057
17.365
17.682
21.713
18.741
23.406
35.108
39.685
41.161
Januar 2018
März 2019

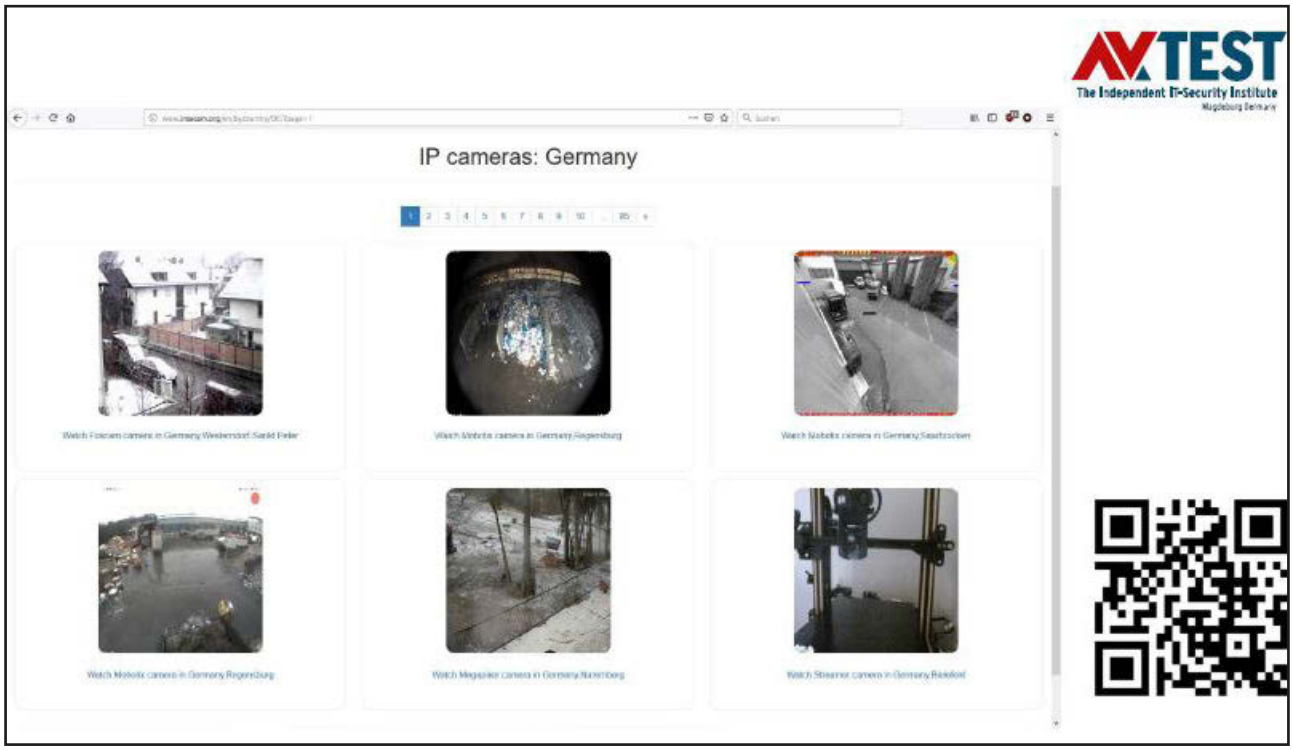

AV-TEST
The Independent IT-Security Institute
Erkennung Linux-Trojaner Tsunami
2
39
20
50
227
168
Juli 2003
Juli 2006
Februar 2010
November 2014
Dezember 2016

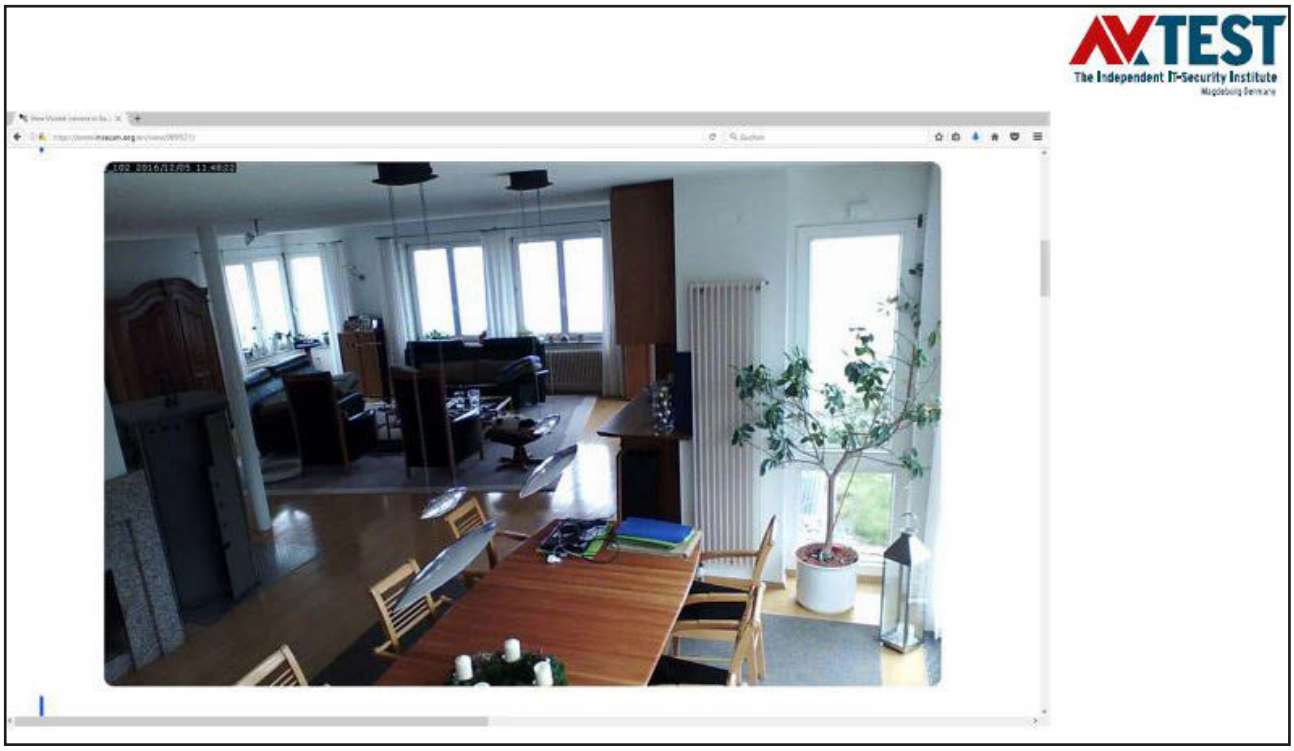

AV-TEST
The Independent IT-Security Institute
Entwicklung Mirai-Bots 2016
2
12
16
13
20
13
7
17.08.2016
06.10.2016
25.10.2016
29.11.2016
06.12.2016
31.12.2016

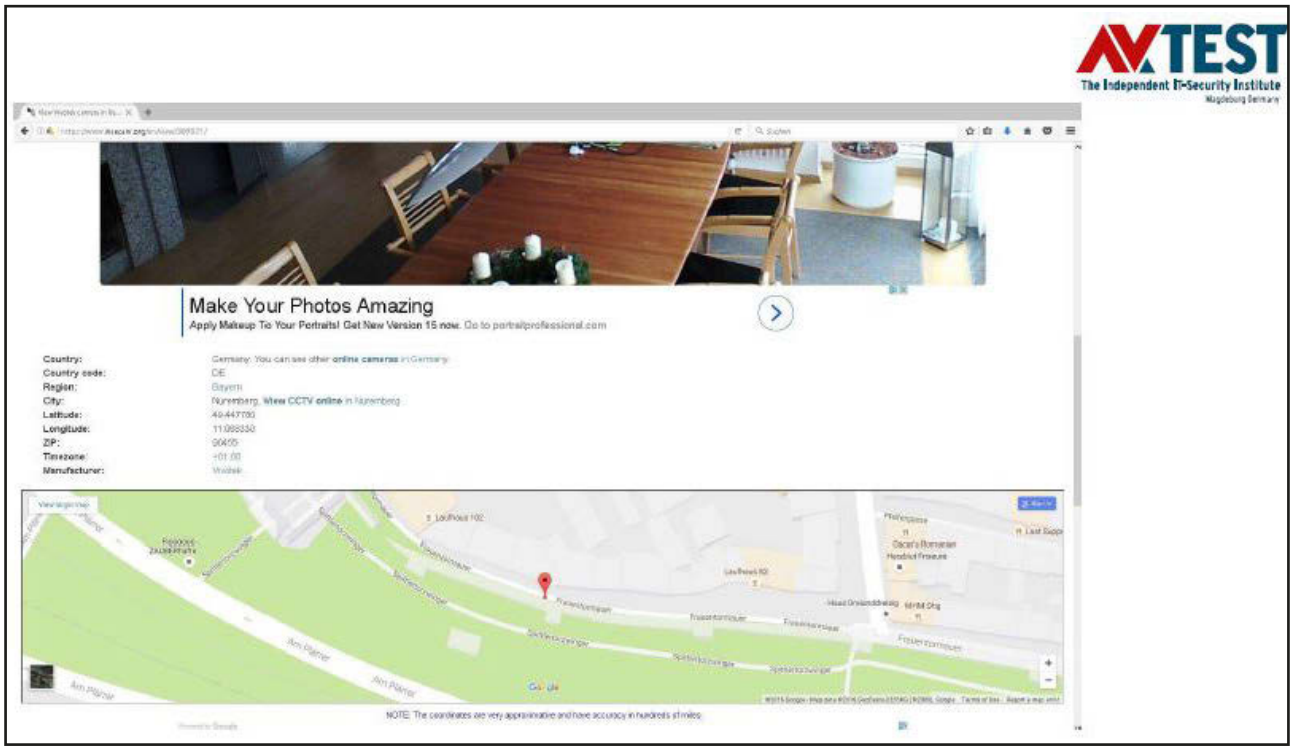

AV-TEST
The Independent IT-Security Institute
Infection Map (age: 6h 45m 23s)
intel.malwaretech.com/botnet/mirai/

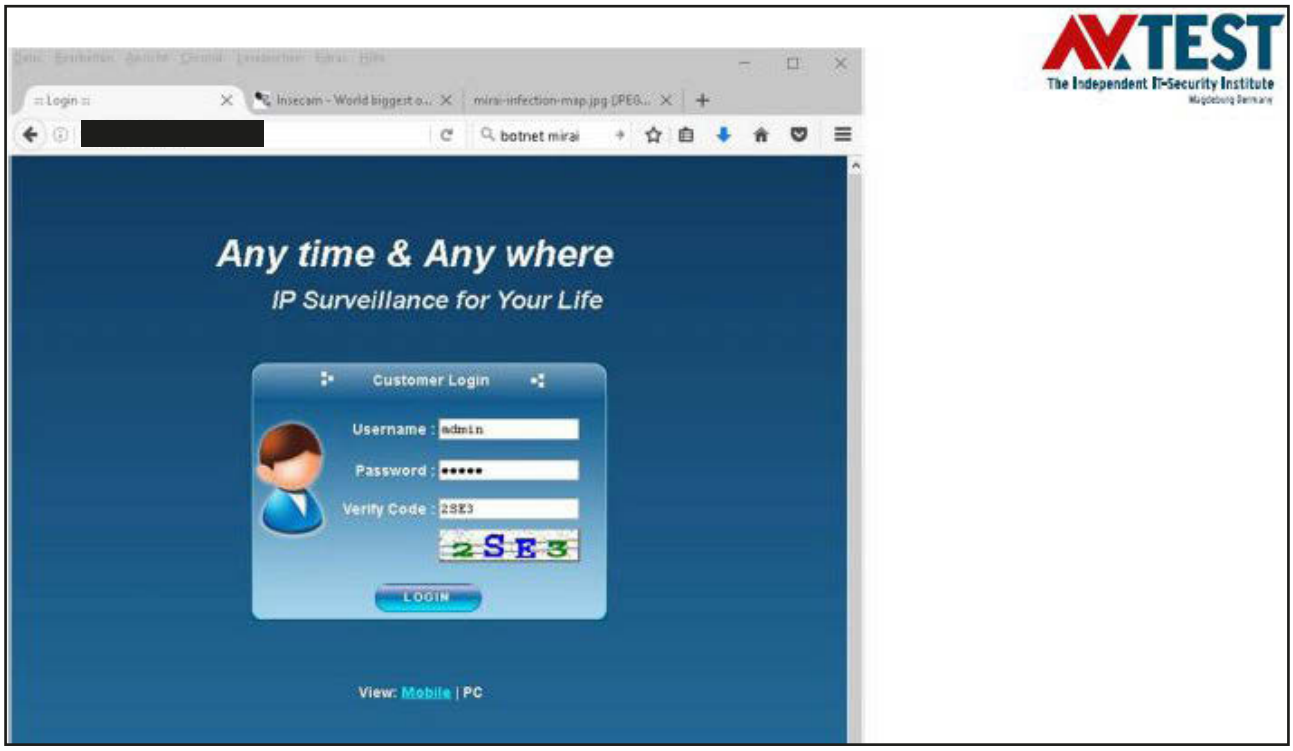

AV-TEST
The Independent IT-Security Institute
IoT: Entwicklung
neuer Mirai-Trojaner 2018 + Q1 2019
14.358
14.532
8.191
6.930
2.388
Januar 2018
August 2018
März 2019


Easy Viewer IP Cam
Quantity of cams to view :
Camera panel size :
CAM SETTINGS
Cam to set :
Cam enable :
Type of cam :
Alias :
IP Adress (DDNS) :
Port :
Login :
Password :
Refresh
Get the latest version here ...
www.easy-herve.com
1 - CAM1
h.nanrocki@yahoo.fr | Easy_Viewer_IP_Cam V1.1
AV-TEST
The Independent IT-Security Institute

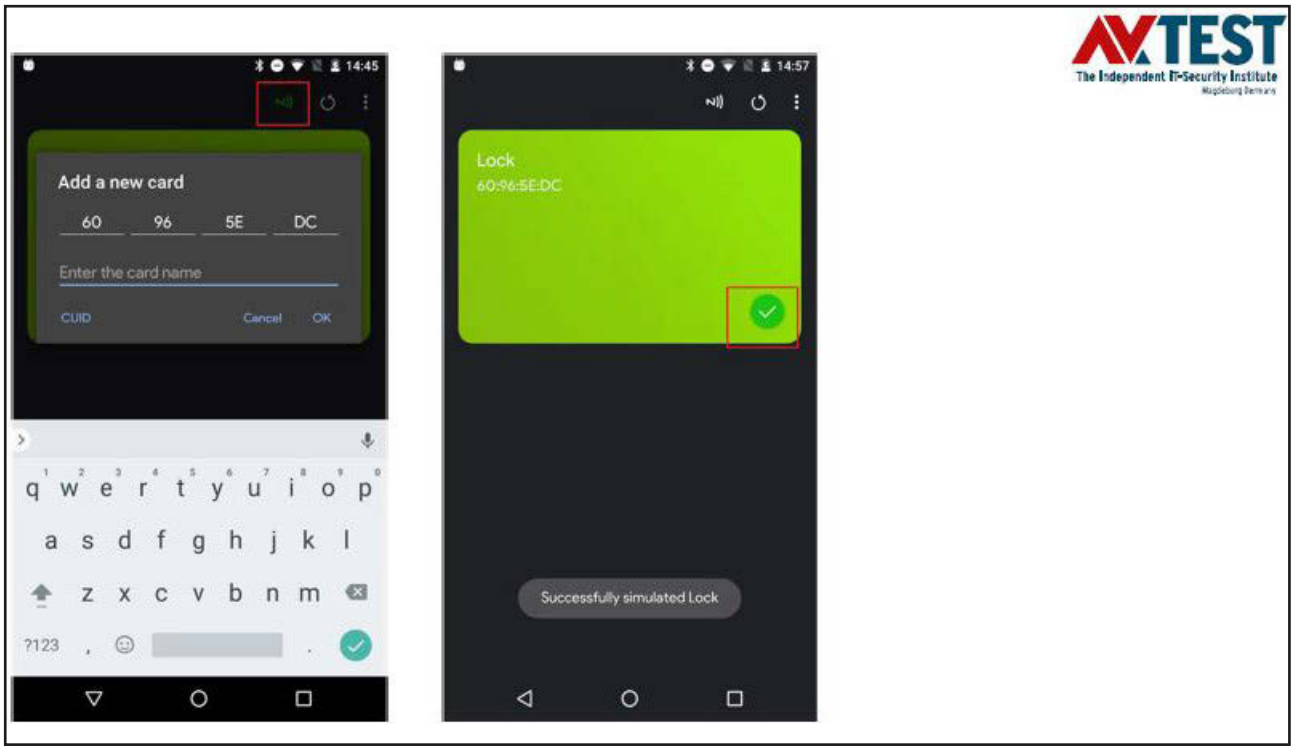

IP cameras: Germany
AV-TEST
The Independent IT-Security Institute


AV-TEST
The Independent IT-Security Institute

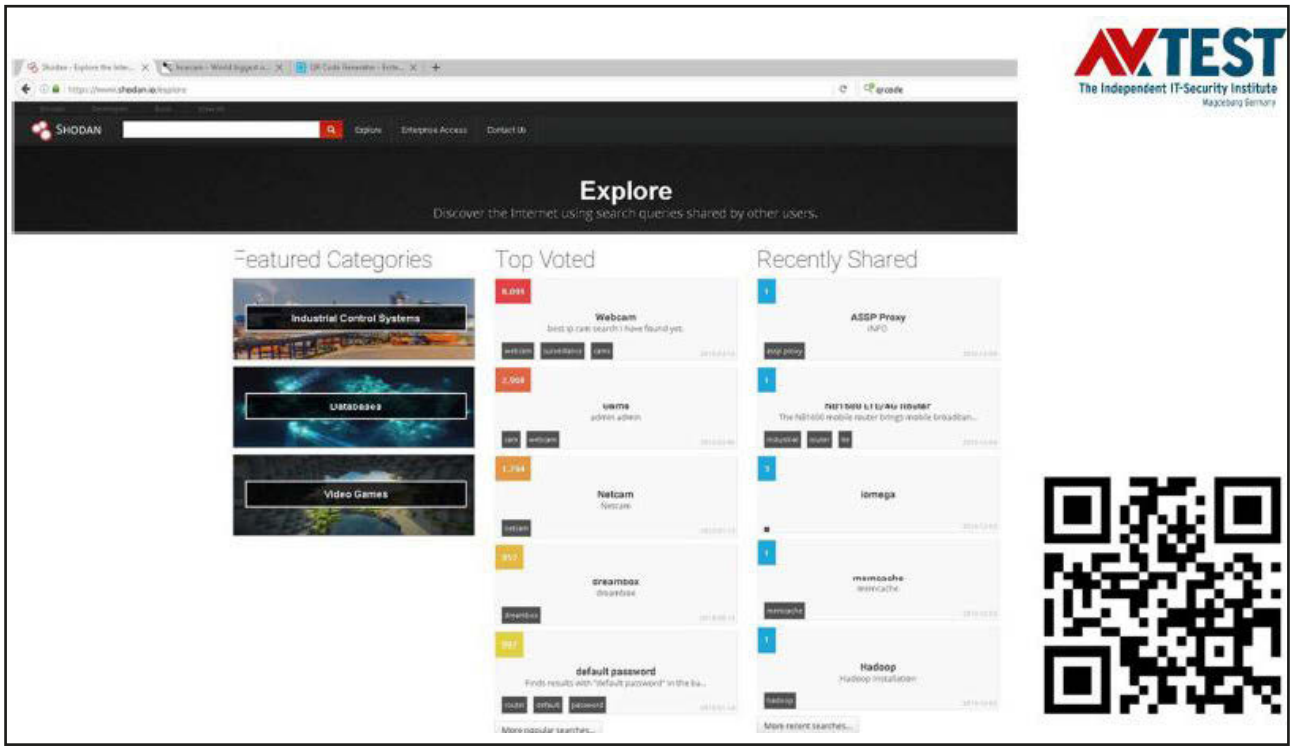

AV-TEST
The Independent IT-Security Institute
Make Your Photos Amazing
Apply Makeup To Your Portraits! Get New Version 15 now.
Country:
Country code:
Region:
City:
Latitude:
Longitude:
ZIP:
Timezone:
Manufacturer:

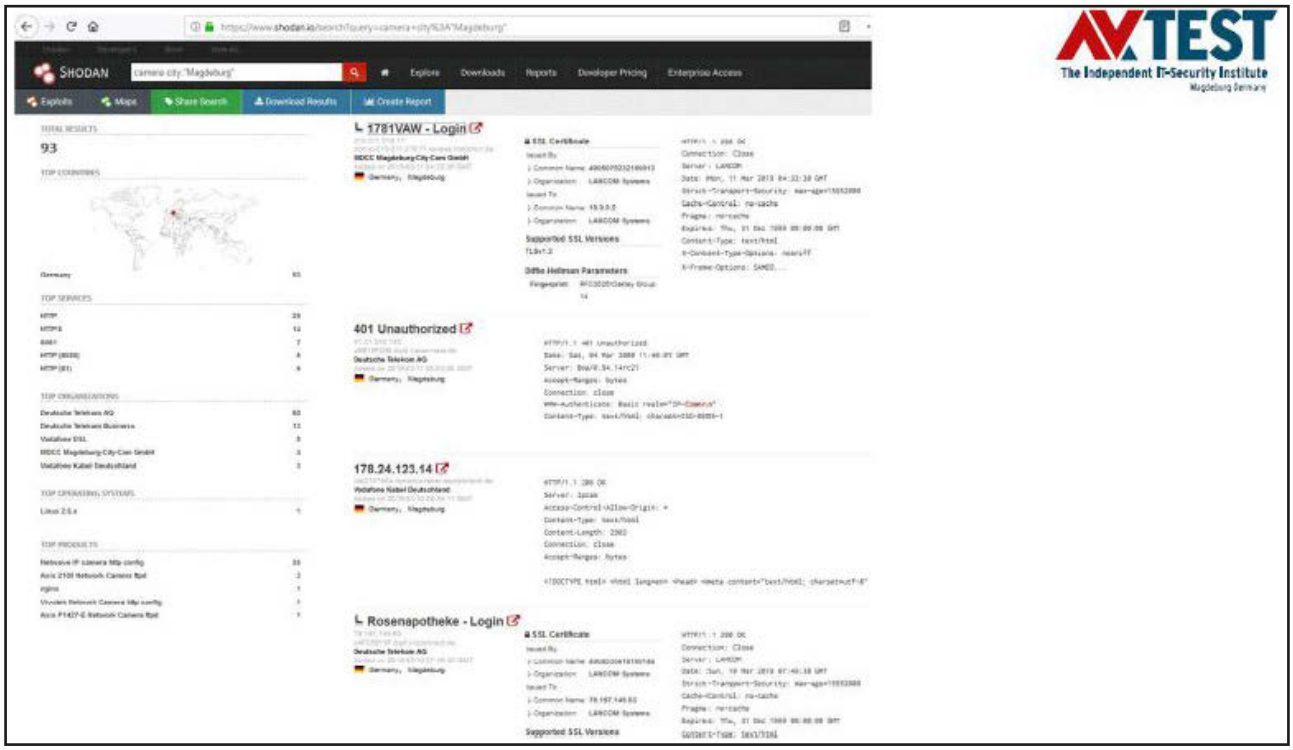

AV-TEST
The Independent IT-Security Institute
botnet mirai
Any time & Any where
IP Surveillance for Your Life
Customer Login
Username : admin
Password :
Verify Code : 2SE3
2SE3
LOGIN
View: Mobile | PC

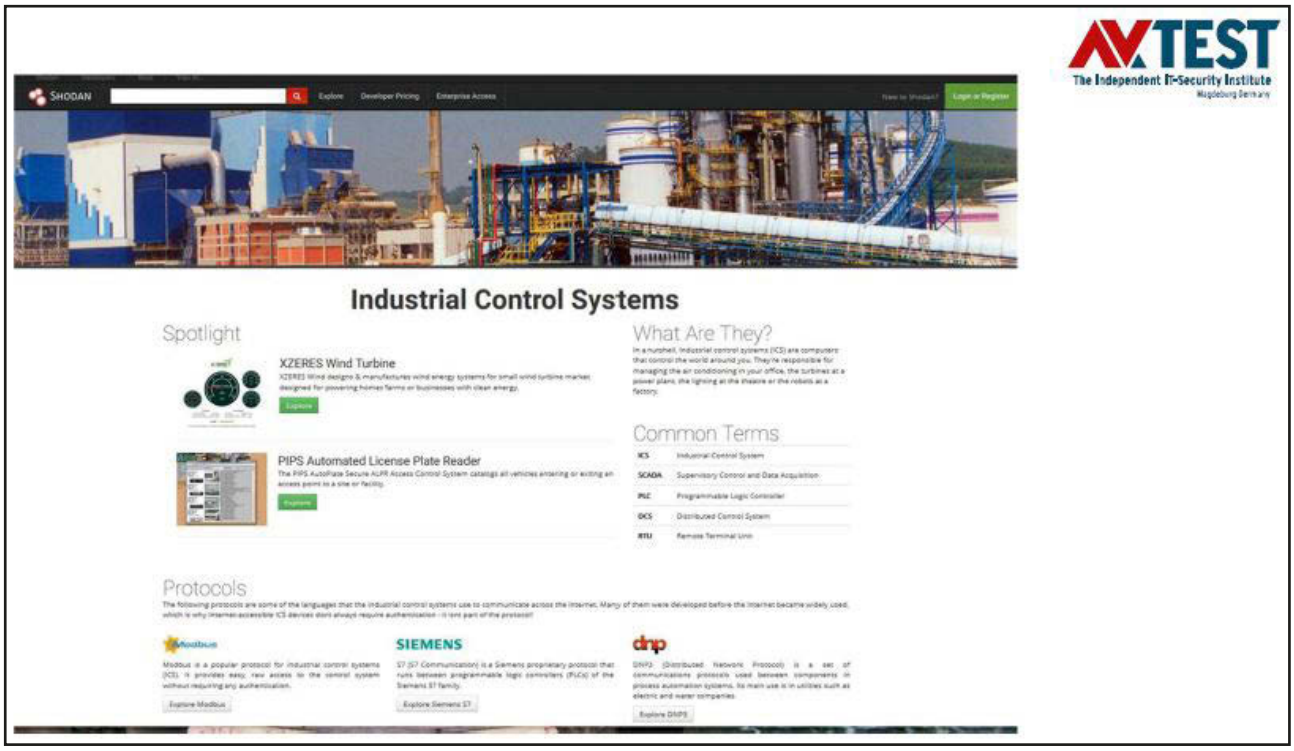

AV-TEST
The Independent IT-Security Institute
POLIZEI


AV-TEST
The Independent IT-Security Institute
Add a new card
60 96 5E DC
Enter the card name
CUID
Cancel
OK
Lock
60:96:5E:DC
Successfully simulated Lock


AV INTERNET OF THINGS BLOG
by AV-TEST
The Independent IT-Security Institute
STARTSEITE
AV-TEST.ORG
Allgemein, Neueste Tests, Smart Home
Pearl Harbor: Sicherheitswarnung für Smartlock VisorTech TSZ-580.fp
August 30, 2019
Olaf Pursche
„Nie wieder ausgesperrt: Denn Sie schließen Ihre Haustür einfach per Fingertipp auf! Alternativ öffnen Sie Ihr Türschloss per Smartphone-App oder Transponder", bewirbt VisorTech sein Smart Lock. Doch leider funktioniert das Öffnen des Smart Locks all zu einfach. Um Türen, in denen das VisorTech-Schloss verbaut ist zu öffnen, brauchen Angreifer nur die unverschlüsselt auf dem mitgelieferten Transponder gespeicherten Zugangsdaten mit einer Gratis-App zu kopieren, schon öffnet das Smartphone fremde Türen. Auf den Hinweis zur Unsicherheit des Transponders durch das AV-TEST Institut hat Pearl mittlerweile reagiert und will neue Schlösser mit Transpondern ausstatten, bei denen die aufgedeckte Sicherheitslücke gefixt wurde. Ob Kunden bisher verkaufter Schlösser informiert werden und sichere Transponder erhalten, lässt der Anbieter auf Nachfrage allerdings offen. Da das VisorTech TSZ-580.fp in puncto Sicherheit auch sonst alles andere als smart ist, hat sich das AV-TEST Institut entschlossen, vor dessen Einsatz zu warnen.
Kategorien
Allgemein
Allgemeine Information
Automobil
eHealth
Gadgets
IP-Kameras
Neueste Tests
Smart Home
Smarte Beleuchtung

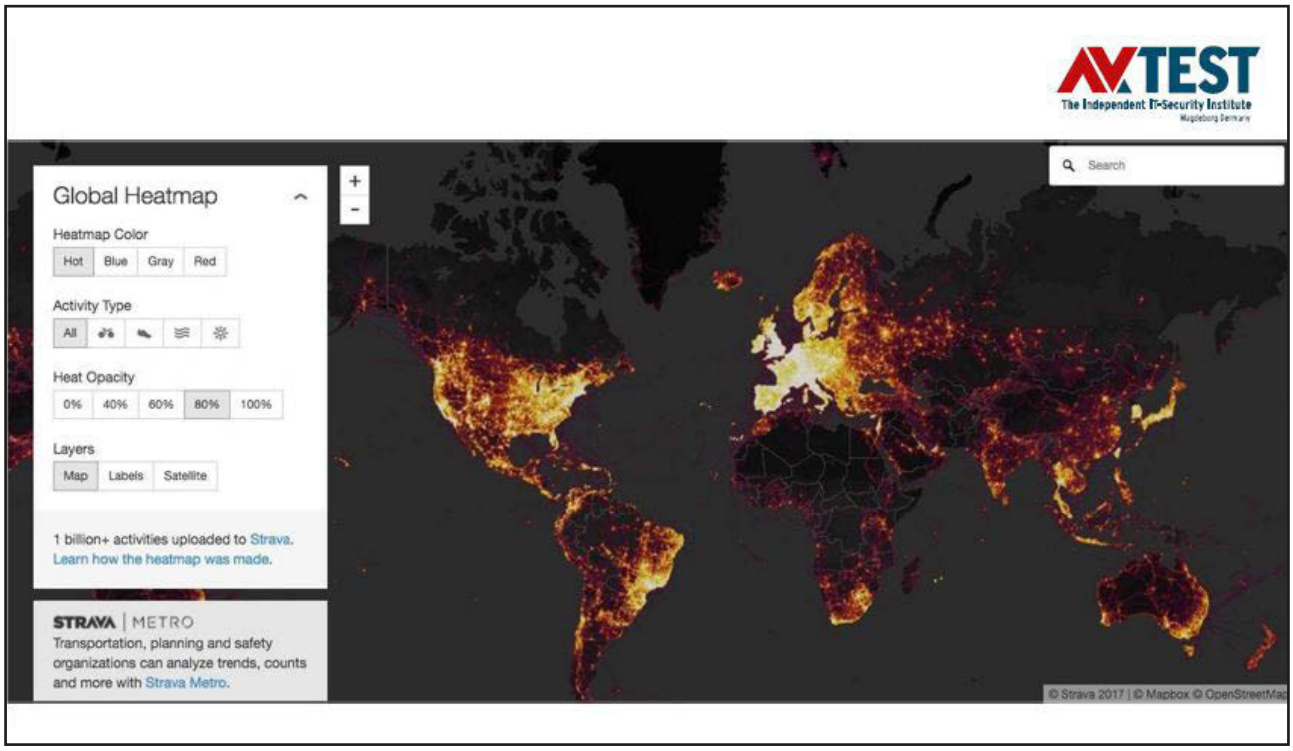

SHODAN
Explore
Enterprise Access
Contact Us
Explore
Discover the Internet using search queries shared by other users.
Featured Categories
Industrial Control Systems
Databases
Video Games
Top Voted
Webcam
Netcam
dreambox
default password
Recently Shared
ASSP Proxy
iomega
memcache
Hadoop


SHODAN
Explore
Downloads
Reports
Developer Pricing
Enterprise Access
Exploits
Maps
Share Search
Download Results
Create Report
93
1781VAW - Login
401 Unauthorized
178.24.123.14
Rosenapotheke - Login

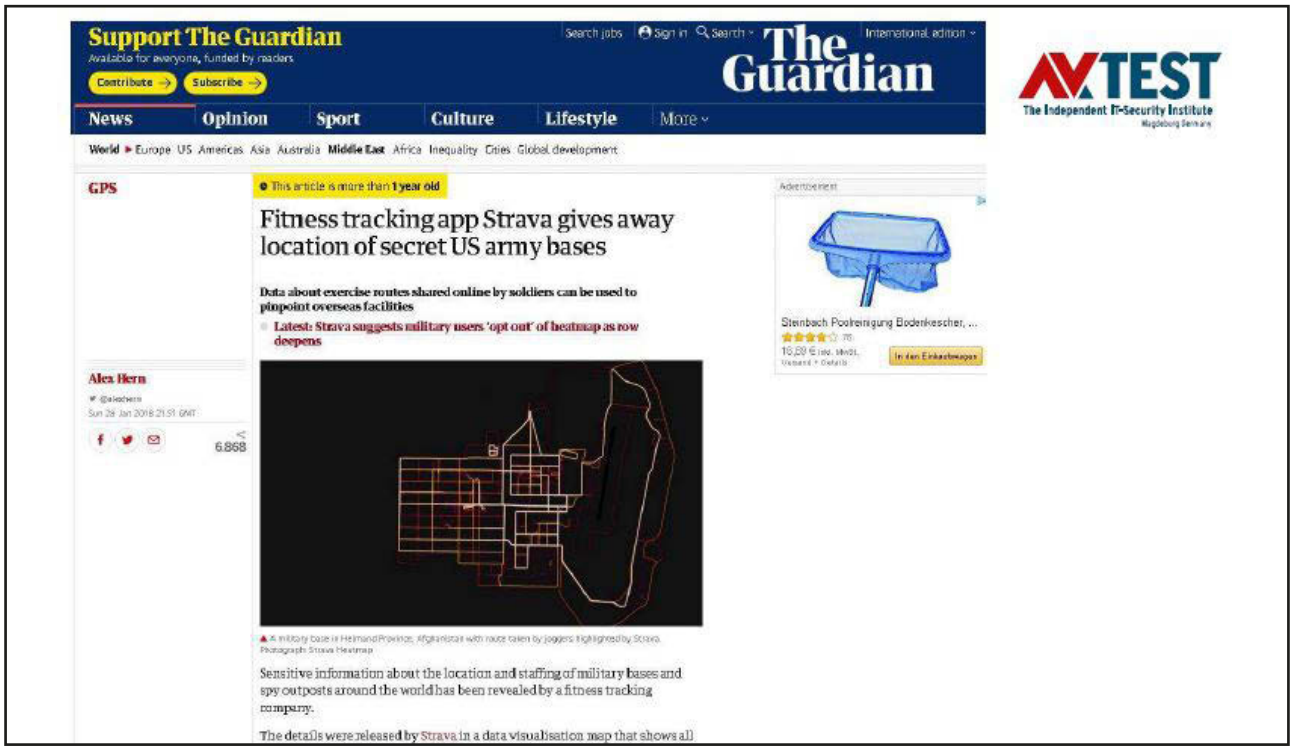

SHODAN
Explore
Developer Pricing
Enterprise Access
Login or Register
Industrial Control Systems
Spotlight
XZERES Wind Turbine
PIPS Automated License Plate Reader
What Are They?
Common Terms
Protocols
SIEMENS
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany


Bürger:
„Ich habe nichts gegen Überwachung. Ich habe schließlich nichts zu verbergen.“
Staat:
„Das weiß ich bereits.“
AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

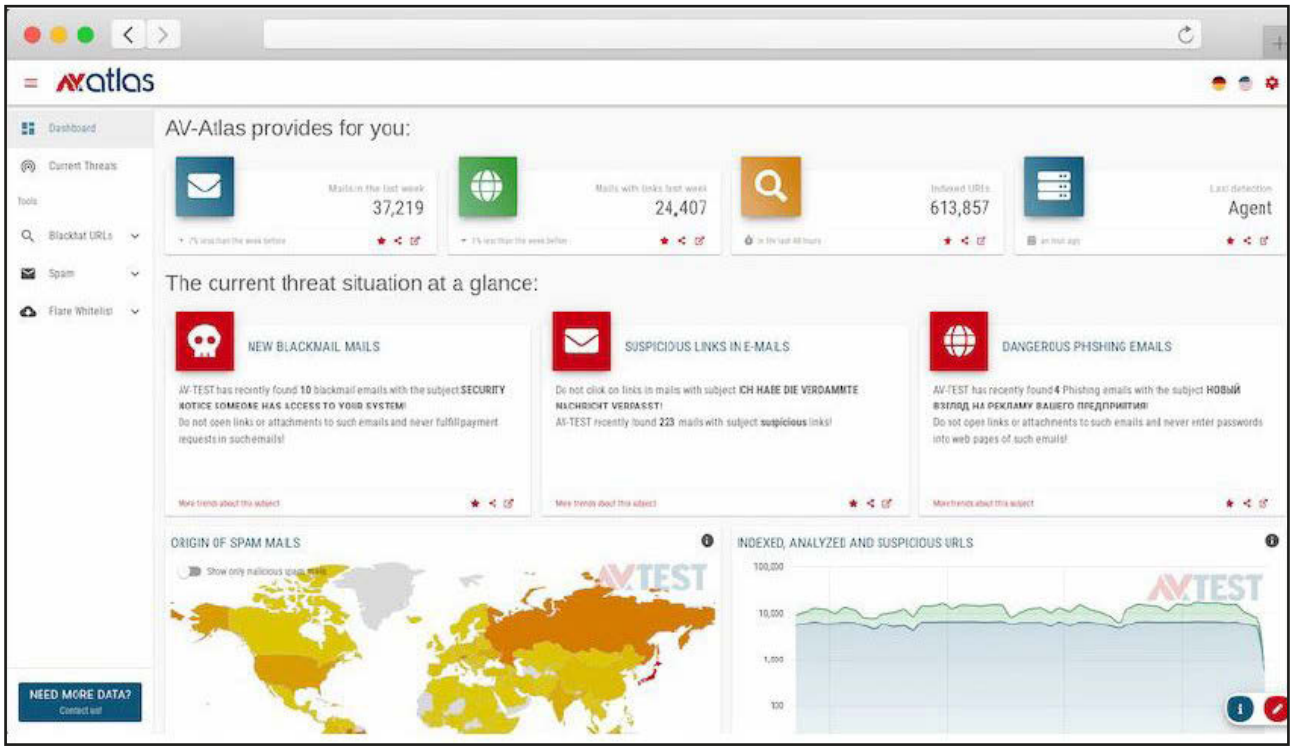

STRAVA
REGISTRIEREN
AV-TEST
The Independent IT-Security Institute
Verbinde dich mit Freunden und teile deine Abenteuer.


AV-TEST
The Independent IT-Security Institute
Global Heatmap
Heatmap Color
Hot
Blue
Gray
Red
Activity Type
All
Heat Opacity
0%
40%
60%
80%
100%
Layers
Map
Labels
Satellite
1 billion+ activities uploaded to Strava.
Learn how the heatmap was made.
STRAVA | METRO
Transportation, planning and safety organizations can analyze trends, counts and more with Strava Metro.
Search
© Strava 2017 | © Mapbox © OpenStreetMap


AV-TEST
The Independent IT-Security Institute
STRAVA LABS
Global Heatmap
STRAVA | METRO
© Strava


Support The Guardian
Contribute
Subscribe
The Guardian
News
Opinion
Sport
Culture
Lifestyle
GPS
Fitness tracking app Strava gives away location of secret US army bases
Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities
Latest: Strava suggests military users 'opt out' of heatmap as row deepens
Alex Hern
Sensitive information about the location and staffing of military bases and spy outposts around the world has been revealed by a fitness tracking company.
The details were released by Strava in a data visualisation map that shows all
AV-TEST
The Independent IT-Security Institute


AV-TEST
The Independent IT-Security Institute
TESTURTEIL
» Sicher «
GEPRÜFTES
SMART HOME
PRODUKT
av-test.org
12/2017
EWE
SCHWAIGER
BOSCH Smart Home
QIVICON
smartfrog
eQ-3
devolo
The Network Innovation


AV-atlas
AV-Atlas provides for you:
37,219
24,407
613,857
Agent
The current threat situation at a glance:
NEW BLACKMAIL MAILS
SUSPICIOUS LINKS IN E-MAILS
DANGEROUS PHISHING EMAILS
ORIGIN OF SPAM MAILS
INDEXED, ANALYZED AND SUSPICIOUS URLS
NEED MORE DATA?


Vielen Dank für Ihr Interesse!
@avtestorg (English) & @avtestde (German)
Folgen Sie uns auf facebook.com/avtestorg
Aktuelle Testergebnisse auf https://www.av-test.org

„Vortrag aus der Digitalwirtschaft“

Marco Langhof
Geschäftsführer Teleport Sachsen-Anhalt GmbH,
Vorsitzender des Verbands der IT-und Multimediaindustrie Sachsen-Anhalt e.V.

Es gilt das gesprochene Wort!

Sehr geehrte Damen und Herren,

ich möchte mich herzlich für die Einladung zum heutigen Wirtschaftsschutztag bedanken und freue mich, zu den Chancen und Risiken der Digitalisierung vortragen zu dürfen.

Fahrplan

Internationalisierung. Es geht nicht mehr ohne.

Digitale Selbstverteidigung? Ein Kräftevergleich.

Internationalisierung. Daheim ist‘s sicherer?

Risikoanalyse. Ein paranoider Ansatz.

Internationalisierung. Ein kleiner Ratgeber für IT-Sicherheit.

Internationalisierung. Geht nicht mehr ohne.

Berührungspunkte:

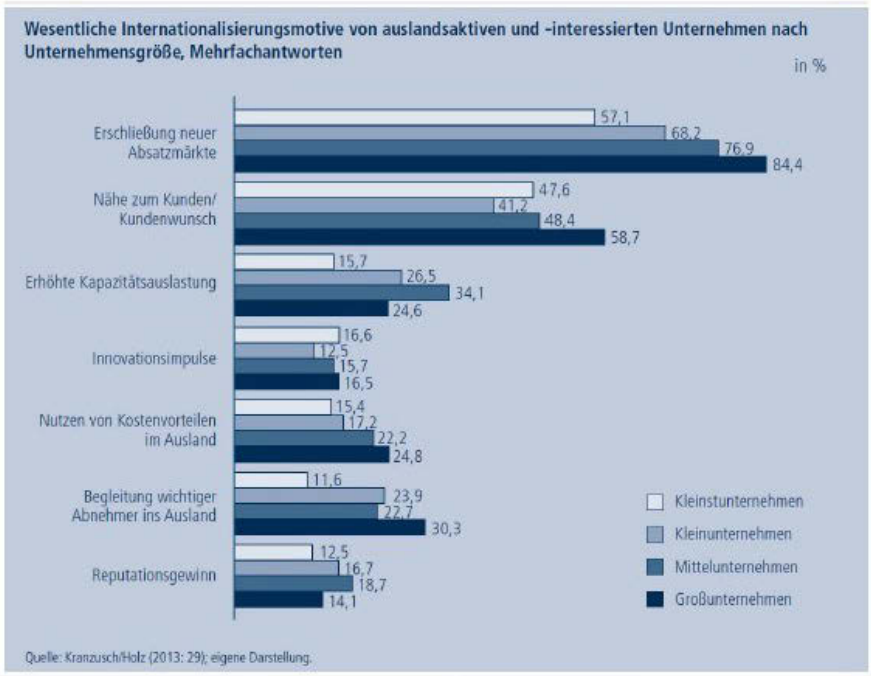
Geschäftsanbahnung / Vertrieb / Absatz von Produkten

Nutzung von Zulieferern / Dienstleistern / Outsourcing / Unternehmenskooperationen / Joint ventures

Indirekte Nutzung von Outsourcing Dienstleistungen (ITK)

After Sales / Service für eigene Produkte

Fachkräfte aus dem Ausland



Fahrplan

Internationalisierung. Geht nicht mehr ohne.

Digitale Selbstverteidigung? Ein Kräftevergleich.

Internationalisierung. Daheim ist‘s sicherer?

Risikoanalyse. Ein paranoider Ansatz.

Internationalisierung. Ein kleiner Ratgeber für IT-Sicherheit.

Digitale Selbstverteidigung? Ein Kräftevergleich.

Digitale Selbstverteidigung? Ein Kräftevergleich.

Die analoge Welt:

Phänomen	Abwehrmöglichkeit
Gewöhnliche Kriminalität von Privatpersonen	Selbstschutz, Wachschutz, Polizei

Digitale Selbstverteidigung? Ein Kräftevergleich.

Die digitale Welt:

Phänomen	Abwehrmöglichkeit
Gewöhnliche Kriminalität von Privatpersonen	Selbstschutz

Läuft am Ende hinaus auf:

...oder:

Fahrplan

Internationalisierung. Geht nicht mehr ohne.

Digitale Selbstverteidigung? Ein Kräftevergleich.

Internationalisierung. Daheim ist‘s sicherer?

Risikoanalyse. Ein paranoider Ansatz.

Internationalisierung. Ein kleiner Ratgeber für IT-Sicherheit.

Internationalisierung. Daheim ist‘s sicherer?

So sicher nicht.

Internationalisierung. Daheim ist‘s sicherer?

Daheim DSGVO einhalten…

…dann klappt‘s auch im Ausland.

Internationalisierung. Daheim ist‘s sicherer?

Hilft die Cloud?
Je kleiner das Unternehmen, desto sicherer die Cloud.

Relativer Sicherheitsabstand der Cloud zu ‚on premise‘ ist größer

- Dediziertes Personal
- Zertifizierte Konzepte
- Bessere Technik
- Bessere Infrastruktur (interkontinentale Redundanz)

Relative Sicherheit der Cloud ist für kleine UN größer

- Angriffs-Wahrscheinlichkeit = 1
- Abwehrwahrscheinlichkeit ist in der Cloud größer (s.o.)
- Wenn Cloud gehackt wird, sind kleine UN das unlukrativere Ziel

Fahrplan

Internationalisierung. Geht nicht mehr ohne.

Digitale Selbstverteidigung? Ein Kräftevergleich.

Internationalisierung. Daheim ist's sicherer?

Risikoanalyse. Ein paranoider Ansatz.

Internationalisierung. Ein kleiner Ratgeber für IT-Sicherheit.

Risikoanalyse. Ein paranoider Ansatz.

Nehmen Sie einfach mal das Schlimmste an...

- Vorsatz und kriminelle Energie
- Kenntnisse über Ihr Unternehmen und seine IT

Stellen Sie sich das Schlimmste vor...

- den maximalen Schaden, der durch ein IT-Sicherheitsproblem oder Betriebssicherheitsproblem ausgelöst werden kann

Sorgen Sie dafür, dass Ihr Unternehmen diese (gedachte) Situation überlebt.

Risikoanalyse. Ein paranoider Ansatz.

Eine Auswahl aus dem ‚Horrorkabinett':

- Blockieren Ihrer Kommunikationskanäle
- Komplettausfall Ihrer IT (Feuer, Diebstahl, Vandalismus)
- Verlust Ihrer Daten
- ‚Abfließen' Ihrer Daten und z.B.
  - Untergraben der Reputation Ihres Unternehmens
  - Kompromittieren Ihrer Kunden
  - Gezieltes Abwerben von Kunden
  - Gezieltes Abwerben von Mitarbeitern
- Störung Ihrer Produktion
- Usw. usf...

Fahrplan

Internationalisierung. Geht nicht mehr ohne.

Digitale Selbstverteidigung? Ein Kräftevergleich.

Internationalisierung. Daheim ist's sicherer?

Risikoanalyse. Ein paranoider Ansatz.

Internationalisierung. Ein kleiner Ratgeber für IT-Sicherheit.

Internationalisierung. Ein kleiner Ratgeber für IT-Sicherheit.

- Ausland ist nicht gleich Ausland
- Sie werden ggf. zum exponierten Ziel
- Gefährdungen sind möglich durch:

  – Wirtschaftsspionage
  – Einsicht in Ihre Daten teilweise regulatorisch möglich
  – Aufspielen von Apps
  – Datenaustausch über unsichere Medien (USB)
  – Kommunikation über unbekannte IT-Systeme und Netze
  – Vortäuschen falscher Identitäten
  – Aufzeichnen kompromittierenden Materials (und nachfolgend Nötigung, Erpressung etc.)
  – Diebstahl von Geräten
  – Beeinträchtigung durch Umgebungsbedingungen

Internationalisierung. Ein kleiner Ratgeber für IT-Sicherheit.

Was können Sie tun?

  – Sicherheitsrichtlinie für Informationssicherheit bei Auslandsreisen
  – Schulung von Mitarbeitern, Sensibilisierung
  – Praktische Maßnahmen wie Sichtschutzfolien, Bildschirmsperre
  – Maßnahmeplan für Verluste von Geräten
  – Sicherer Remote-Zugriff bzw. sichere Nutzung von WLANs (VPN)
  – Sicherer Umgang mit mobilen Datenträgern
  – Verschlüsselung von mobilen Geräten und Datenträgern
  – Diebstahlsicherung
  – Sicheres Vernichten von Dokumenten und Materialien

Internationalisierung. Ein kleiner Ratgeber für IT-Sicherheit.

Was können Sie noch tun?

- Minimierung der Datenmitnahme
- Datenverschlüsselung
- verschlüsselte Mail-Kommunikation
- ggf. abstrahlsichere Geräte verwenden
- Datenintegrität sichern (digitale Signaturen nutzen)
- Dedizierte Reise-Hardware
- Eingeschränkte Berechtigungen während Auslandsreisen

Grundlagen

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_7_Informationssicherheit_auf_Auslandsreisen.html

Noch ein paar IT-Aspekte der Internationalisierung

IT-Anforderungen bestehen auch in verschiedenen anderen Richtungen:

- andere regulatorische Bedingungen
- Mehrsprachenfähigkeit
- Währungsfähigkeit
- Regionale Besonderheiten (Anforderungen an Buchungsbelege in China)
- Steuerfragen (z.B. Berechnung der Umsatzsteuer in den USA)

Wie Sie sehen:

IT-Sicherheit ist nicht alles –

aber ohne IT-Sicherheit ist alles nichts!

Vielen Dank für Ihre Aufmerksamkeit

Wenn

- Sie in Kontakt mit leistungsfähigen IT-Unternehmen treten möchten und
- Sie den Eindruck hatten, wir wüssten wovon wir sprechen...

...finden Sie hier kompetente Ansprechpartner:

Verband der IT- und Multimediaindustrie
Sachsen-Anhalt e. V.

im HAUS DER WIRTSCHAFT
Humboldtstraße 14
39112 Magdeburg

„Die Digitalisierung und ihre Bedrohungen aus Sicht des BSI“

Ariane Steinke

Leiterin Regionalbüro Nord,
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Es gilt das gesprochene Wort!

Meine sehr verehrten Damen und Herren,
mit dem Vortrag gibt das BSI einen Einblick in die Herausforderung der Cybersicherheit in der Digitalisierung. Anhand des Beispiels der Industrie 4.0 wird aufgezeigt, welche Bedrohungspotentiale und Chancen aus der fortschreitenden Digitalisierung mit ihren Elementen der Vernetzung, Komplexität und Allgegenwertigkeit erwachsen.
Auf die Frage: „Wie bedroht ist Deutschlands Cyber-Raum?“ wird mit Zahlen aus dem Lagebericht zur IT-Sicherheit in Deutschland 2019 geantwortet. Am Beispiel ausgewählter Cyber-Sicherheits-phänomene werden aktuelle Trends und Entwicklungen aufgezeigt. Mit der Vorstellung der Ergebnisse einer Online-Umfrage der „Allianz für Cybersicherheit“ wird die Betroffenheit der Wirtschaft in den Fokus gerückt.


Das BSI – vernetzte Kompetenzen in der Cyber-Sicherheit
Nachhaltigkeit
Erkennen der Schwachstelle
Strategisches Lagebild
Anpassen der Vorgaben und der Produkte
Prävention
Detektion
BSI
Reaktion
Erkennen des Angriffs
Koordination der Cyber-Abwehr
Bewältigen des Cyber-Angriffs
Bewerten des Cyber-Angriffs


Cyber-Sicherheit in der Digitalisierung
Vernetzung
Komplexität
Allgegen-wärtigkeit
Digitalisierung bedeutet…
…mehr Möglichkeiten,
auf die Deutschland nicht verzichten kann und soll
…mehr Gefahren,
auf die Deutschland vorbereitet sein muss
Cyber-Sicherheit
…unverzichtbare Voraussetzung für das Gelingen der Digitalisierung
Bundesamt für Sicherheit in der Informationstechnik

Smart Factory / Industrie 4.0

© zapp2photo – Fotolia.com

© Mimi Potter – Fotolia.com

Bundesamt für Sicherheit in der Informationstechnik

Alle Lagebilder teilen ein Problem

Bild: © niyazz – Fotolia.com

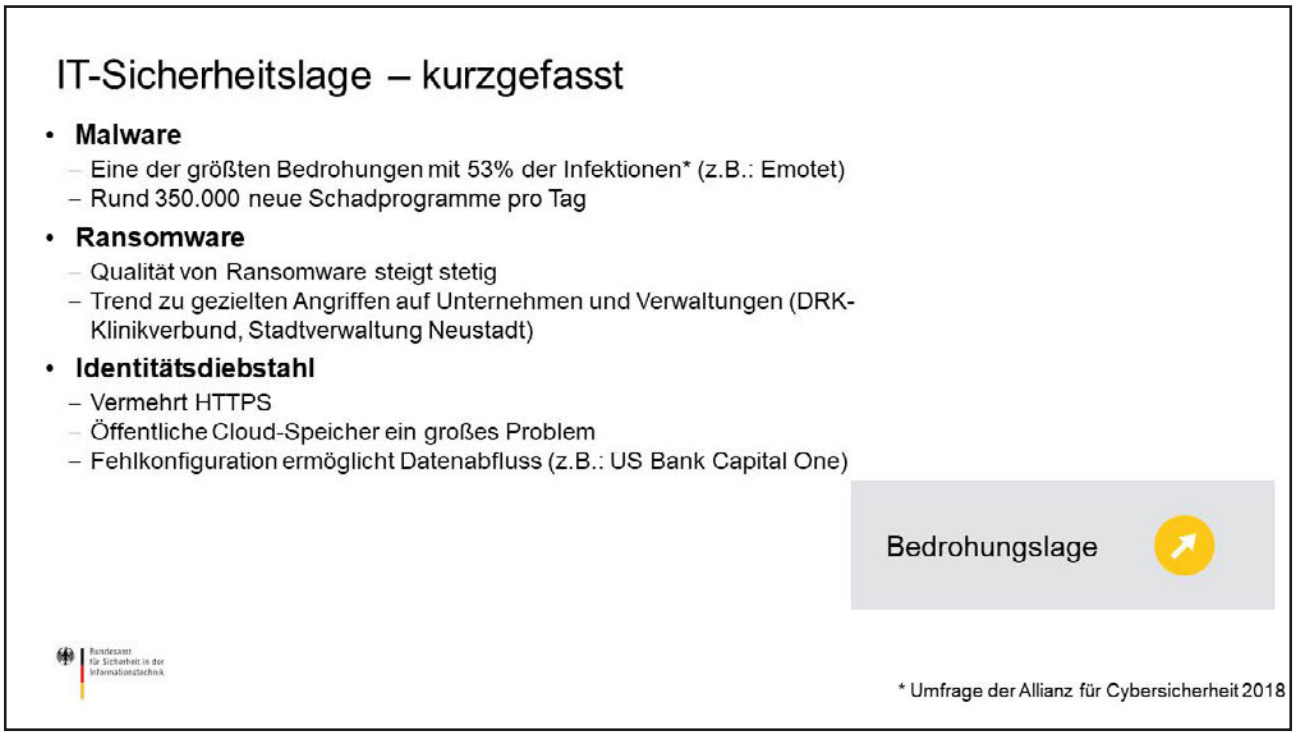
Bundesamt für Sicherheit in der Informationstechnik

Wie bedroht ist Deutschlands Cyber-Raum?

- **Neue Angriffsqualität** hebt die Gefährdungslage auf ein neues Niveau und **erfordert flexible Gegenmaßnahmen** auf Seiten der Verteidiger.
- Bei Angriffen auf die Bundesverwaltung wurden rund **770.000 E-Mails mit Schadsoftware** abgefangen.
- **11,5 Millionen Meldungen zu Schadprogramm-Infektionen** hat das BSI an deutsche Netzbetreiber übermittelt.
- Bis zu **110.000 Botinfektionen täglich** konnten in deutschen Systemen festgestellt werden.
- Rund **114 Mio. Variationen von neuen Schadprogrammen** wurden im Berichtszeitraum gesichtet.
- **DDoS-Angriffe mit bis zu 300 Gbit/s** wurden in Deutschland detektiert.
- **Vorinstallierte Schadsoftware** wurde auf IT-Geräten gefunden.

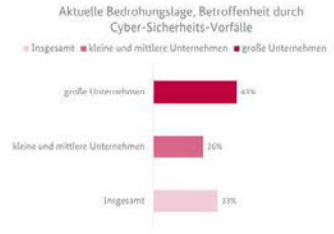
Quelle: BSI

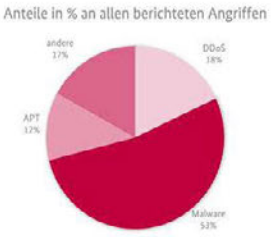
Top 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	↗
Infektion mit Schadsoftware über Internet und Intranet	↗
Menschliches Fehlverhalten und Sabotage	↑
Kompromittierung von Extranet und Cloud-Komponenten	↑
Social Engineering und Phishing	↘
(D)DoS Angriffe	↑
Internet-verbundene Steuerungskomponenten	→
Einbruch über Fernwartungszugänge	→
Technisches Fehlverhalten und höhere Gewalt	↘
Kompromittierung von Smartphones im Produktionsumfeld	→

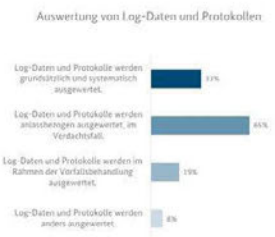

IT-Sicherheitslage – kurzgefasst
• Malware
– Eine der größten Bedrohungen mit 53% der Infektionen* (z.B.: Emotet)
– Rund 350.000 neue Schadprogramme pro Tag
• Ransomware
– Qualität von Ransomware steigt stetig
– Trend zu gezielten Angriffen auf Unternehmen und Verwaltungen (DRK-Klinikverbund, Stadtverwaltung Neustadt)
• Identitätsdiebstahl
– Vermehrt HTTPS
– Öffentliche Cloud-Speicher ein großes Problem
– Fehlkonfiguration ermöglicht Datenabfluss (z.B.: US Bank Capital One)
Bedrohungslage
Bundesamt für Sicherheit in der Informationstechnik
* Umfrage der Allianz für Cybersicherheit 2018


IT-Sicherheitslage – kurzgefasst
• DDoS
– Multivektor-Angriffe und DDoS aus der Cloud
– Immer wieder Werte von >150Gbit/s
– Aktuelles Beispiel: DDoS auf Wikipedia, September 2019
• Schwachstellen (Hardware)
– Meltdown/Spectre (versch. Varianten), Zombieload (Mai 2019), RamBleed (Juni 2019)
Bedrohungslage
Bundesamt für Sicherheit in der Informationstechnik

Fokus „Wirtschaft“







Bundesamt für Sicherheit in der Informationstechnik

Öffentliche Online-Umfrage auf www.allianz-fuer-cybersicherheit.de von 1039 teilnehmenden Organisationen von 21.2.2019 – 7.3.2019

Zusammenfassung: IT-Sicherheitslage

- Fortlaufende Betroffenheit von Staat, Wirtschaft und Gesellschaft in Deutschland
- Dimension der Cyber-Angriffe in D ist besorgniserregend.
- Neue Angriffsqualität und zunehmende Digitalisierung erfordern nachdrückliche Maßnahmenumsetzungen

Bundesamt für Sicherheit in der Informationstechnik

„Herausforderung CyberSecurity – der CyberSecurity-Verbund Sachsen-Anhalt“

Prof. Dr. Hermann Strack,
Hochschule Harz (HS Harz)
Dr. Sandro Wefel,
Martin-Luther-Univ. Halle/Wittenberg (MLU)
Stefan Kiltz,
Otto-von-Guericke Universität (OvGU)

Prof. Dr. Hermann Strack

Es gilt das gesprochene Wort!

Sehr geehrten Damen und Herren,

Informationssicherheit (Security) und Datenschutz stellen wichtige Themen für KMU und Verwaltungen dar, deren Nichteinhaltung zu Bedrohungen und rechtlichen Sanktionen führen kann, wenn gegen entsprechende Gesetze und Verordnungen verstoßen wird. Die Umsetzung der Anforderungen an IT- und Datensicherheit sowie technischen Datenschutz sind allerdings herausfordernd und aufwändig. Sie sind nur schwer durch kleinere Unternehmen ohne Beratung und Begleitung umzusetzen. Um dieser Problematik effektiv zu begegnen, ist es notwendig, die wissenschaftlichen Kapazitäten des Landes Sachsen-Anhalt im Bereich Informationssicherheit und Datenschutz (ggf. auch Verbraucherschutz) entsprechend zu bündeln und somit diese Querschnittsziele der Digitalen Agenda des Landes Sachsen-Anhalt auch aus der Wissenschaft effektiv zu unterstützen.

Mit der Frage, wie Unternehmen und öffentliche Einrichtungen ihre Daten, Netzwerke und digitalen Prozesse besser vor Cyber-Angriffen schützen können, beschäftigt sich ein neues Forschungsverbundprojekt von Informatikern und IT-Experten der Hochschule Harz, der Martin-Luther-Universität Halle-Wittenberg und der Otto-von-Guericke-Universität Magdeburg. Durch Austausch und wechselseitigen Zugriff auf Kenntnisse und technische Einrichtungen der Partner bietet die Zusammenarbeit im Verbund mehr Möglichkeiten, als die ansonsten verteilt arbeitenden IT-Sicherheitsbereiche der beteiligten Hochschulen.

Die zunehmende Digitalisierung stellt Sicherheitsexperten vor große Herausforderungen:
Informationstechnik wird oft im Laufe der Zeit im Selbstbau-Verfahren aus Angeboten verschiedenster Anbieter „aus dem Regal“ zusammengestellt. Dabei mangelt es dann oft an der Integration einer soliden gemeinsamen Sicherheitsarchitektur solcher IT-Verbunde und deren weiteren Pflege durch ein konsequentes Sicherheitsmanagement. Deshalb braucht es neue Ansätze, mit denen Unternehmen und Einrichtungen der öffentlichen Hand weiterhin zeitgemäß arbeiten und trotzdem ihre Daten, Systeme und digitalisierten Prozesse proaktiv integriert schützen können.

Gemeinsam im Verbund sollen unter anderem folgende Themen angegangen werden (exemplarische Aufzählung):
Informationssicherheits-Integration für Infrastrukturen, Sicherheitsmanagement,

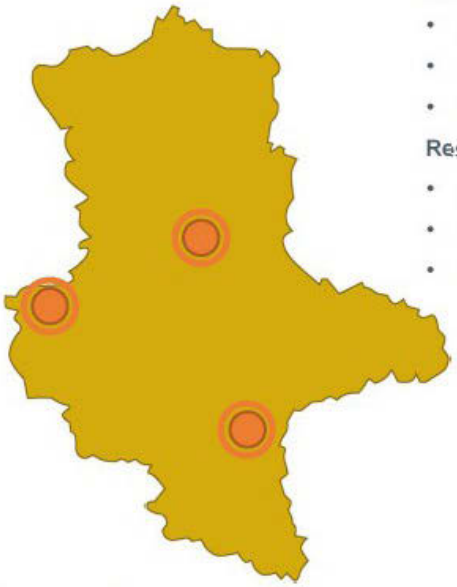
Security-by-Design, Netzwerksicherheit, Anwendung und Integration von Sicherheits- und E-Government-Standards, Security-Prototyping, -Analysen und -Labortests sowie Transfer zu Industrie 4.0 und IOT (Internet of Things), Integration kryptografischer Schutzmaßnahmen in Verfahrensabläufe und kritische Infrastrukturen. Auch die Themen digitale & digitalisierte Medien-, Netzwerk- und Computer-Forensik sowie Tatortforensik werden eine Rolle spielen.

Die Kernaufgaben des Verbundes sind die Beratung und die wissenschaftliche Begleitung sowie die Fort- und Weiterbildung für Unternehmen und öffentliche Verwaltungen, insbesondere auch Schulen, zu Fragen und realisierbaren Lösungen in den Bereichen IT-Sicherheit und technischer Datenschutz sowie der Bildung in diesen Bereichen.

Agenda

- Motivation / Vorfälle
- Security-Aufgabe – Awareness & Herausforderungen
- CyberSec-LSA – Projekt, Kompetenzen und Tasks
- F&E: Aktuelles und Vorarbeiten
- Security als Wirtschaftszweig - Unterstützung F&E

CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE



Faculties/Institutes/Research Groups:

- Automation and Computer Science (HZU)
- Institute for Computer Science (MLU)
- Arbeitsgruppe Multimedia and Security (OvGU, AMSL)

Research Cooperation at IT-Security

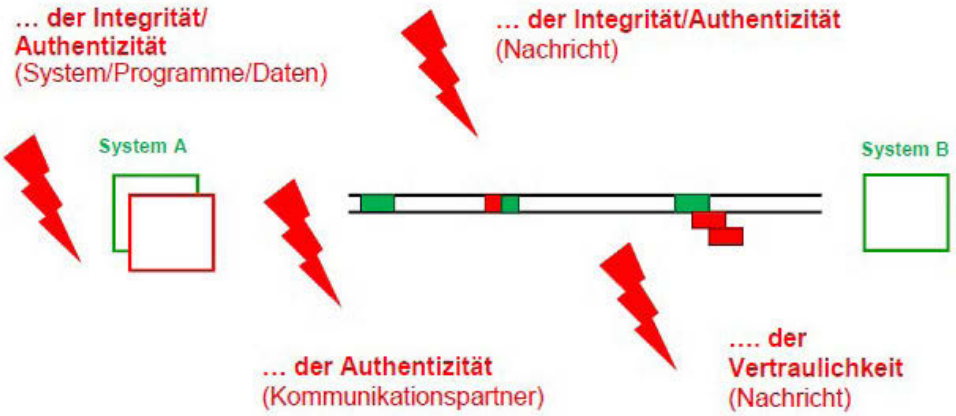
- IT-Security (Saxony-Anhalt) research and cooparation
- Federal State & Local State (Saxony-Anhalt) Funding
- Application for EU Funding

CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE


Motivation & Vorfälle
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE


Motivation / Vorfälle
Verstärkte / verschärfte IT-Bedrohungslage auch in Deutschland, z.B.:
Bundestagsangriff
Mio.-fache Mailkonten-Angriffe (…2019)
Industrieattacken, Botnetze
Ransomware-Attacken existentiell
Kein Anlass mehr für: …mich trifft es schon nicht, etwas Security reicht schon, Hauptsache „Digitalisierung“
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

Bedrohung von Netzen & IT-Systemen



CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

Motivation / Vorfälle

Ransomware
WannaCry/Emotet:

- Verschlüsselt Dateien/Dateisysteme („erpresst Lösegeld“)
- Bekannt für den Befall von Krankenhäusern, Auftreten Mitte Mai 2017 – 2019 (BSI)
- Patches relativ zügig verfügbar, aber noch Neuinfektionen/Altlasten

CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE


Aufgaben, Awareness & Kompetenzen
• Mindest-Qualifikation zu Security, rollen-bezogen, als notwendiger Bestandteil von IT-Medien- & Management-Kompetenz (inkl. awareness)
• konzeptionelle Security-Unterstützung insb. für KMU & Verwaltungen
• bekannte (fundamentale) Schwachstellen von Default-IT konstruktiv verbessern (z.B. Defizite SW-Update-Fähigkeit, Separierungen, ungeeignete Zugriffskontrollen für SW-Management, eID/Authentisierungen,…)
• Security-Verstärkungen oft F&E-nah (z.B. Architekturen/Komponenten, Krypto-Einsatz, komplexe Testbeds, „Security by Design“ für IT-Spezialisten, Zuarbeiten zu Sec.-Evaluierung & Zertifizierung für Vertrauenswürdigkeit …)
• => Security als HiTec- & Wirtschafts-Förderung 5.0
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE


CyberSec-LSA-Vorstellung:
Kompetenzen & Tasks
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

Wiss. CyberSecurity-Verbund CyberSec LSA

Bündelung der wiss. Security-Kräfte LSA (EFRE, Digitale Agenda LSA):

KAT InnoLab SecInfPro / netlab (Hochschule Harz)

- CyberSec-LSA-HS-Harz: Komponenten-basierte Security-Integrationen per Security-By-Design/Management für Wirtschaft und Verwaltung
- Prof. Dr. Strack & Team

ITSecLab (Institut für Informatik der Universität Halle-Wittenberg)

- CyberSec-LSA-MLU: Embedded-System-Security und Kryptographie Prof. Dr. Molitor / Dr. Wefel & Team

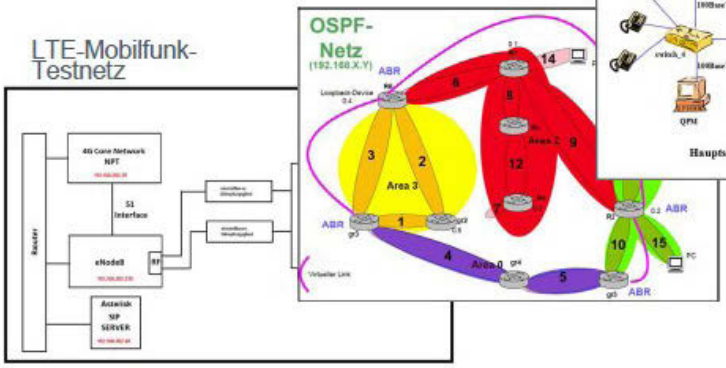
Arbeitsgruppe Multimedia and Security (Otto-von-Guericke-Univ. Magdeburg)

- CyberSec-LSA-OVGU-AMSL: Security-by-Design-Orchestrierung
- Prof. Dr. Dittmann & Team

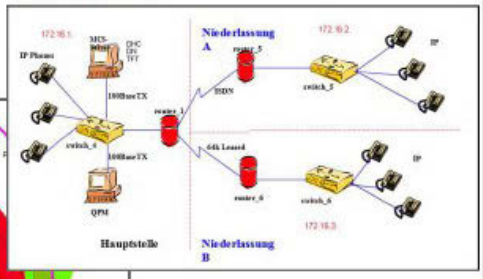
CYBER | SEC · MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG · OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG · Hochschule Harz · SACHSEN-ANHALT · EFRE

Impressionen netlab HS Harz - Netzwerktechnik

Routing

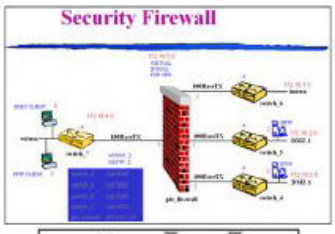


Voice over IP

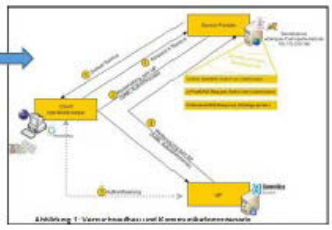


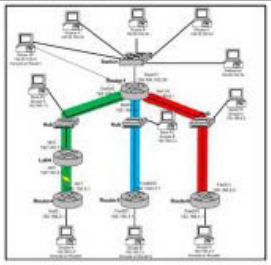
CYBER | SEC · MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG · OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG · Hochschule Harz · SACHSEN-ANHALT · EFRE

Netlab HS Harz - Impressionen: IT-Sicherheit



Neuer Personalausweis &
eID-Service / eIDAS





Netzwerksicherheit mit VPNs

KAT SecInfPro-Geo, mobil

Lehrintegration: Bachelor/Master, Fort/Weiterbildung (IEA)

CYBER | SEC

MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Hochschule Harz

SACHSEN-ANHALT

EFRE

eGovernment, IT-Sicherheit, Prozesselektronisierung (F&E)

Kurzübersicht Projekte ÖV (2010 - 2019, netlab):

- eCampus/Scampii – Kultusministerium /MW LSA/EU-EFRE
- SecInfPro/Kompetenzzentrum – Min. Wissenschaft & Wirtschaft LSA
- eGov.-Initiative neuer Ausweis/eID – BMI 2012/2013
- eID an Hochschulen (Hs Harz u. MLU) – MW u. ITKOM LSA 2015
- **eIDAS eID für Hochschulprozesse, TREATS/eIDAS-Verbund (EU CEF, Governikus… et.al.)**
- **eIDAS eID & eSignature für Hochschulprozesse StudIES+/eIDAS (EU CEF) -> z.B. OZG/eZeugnis**

Co-financed by the European Union
Connecting Europe Facility

StudIES+

CYBER | SEC

MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Hochschule Harz

SACHSEN-ANHALT

EFRE

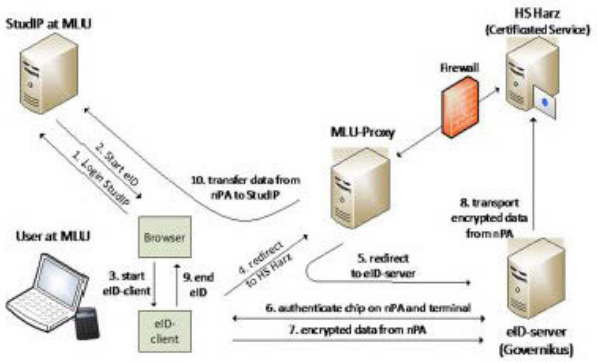
▲ Hochschule Harz
Hochschule für angewandte Wissenschaften
Harz University of Applied Sciences

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

Vorarbeiten eID-Test Cross Domain:

eID-Proxy MLU/HS Harz

- technische Integration:
  - Proxy-Konzept Dienste
  - Sec.-Schalenarchitektur
- juristische Integration:
  - Anpassungen HochschulGesetze



CYBER | SEC

MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

▲ Hochschule Harz

SACHSEN-ANHALT

EFRE

Forschung

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

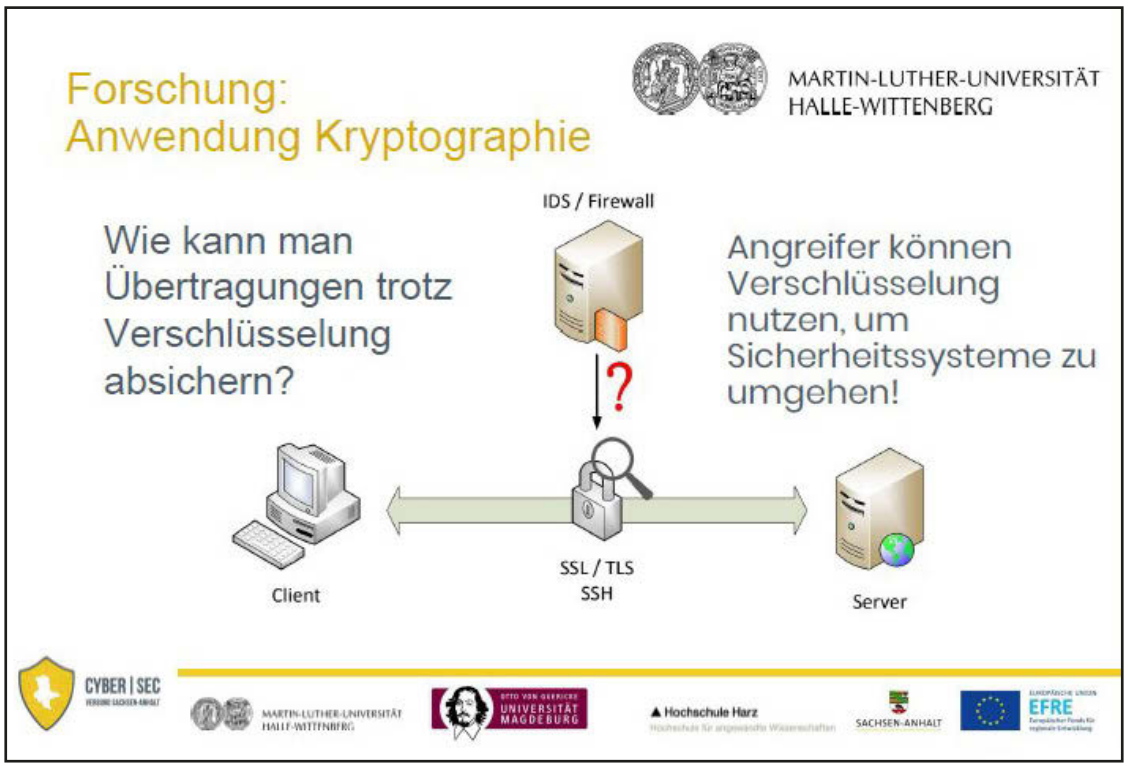
- Aufbau sichererer **Authentisierungsverfahren**
- Anwendung **kryptographischer Maßnahmen**
- Untersuchung Netzwerkprotokolle
  - **Verschlüsselte Kommunikation**
- Absicherung der (Funk-) **Datenübertragung**, z.B. für **IoT-Geräte**

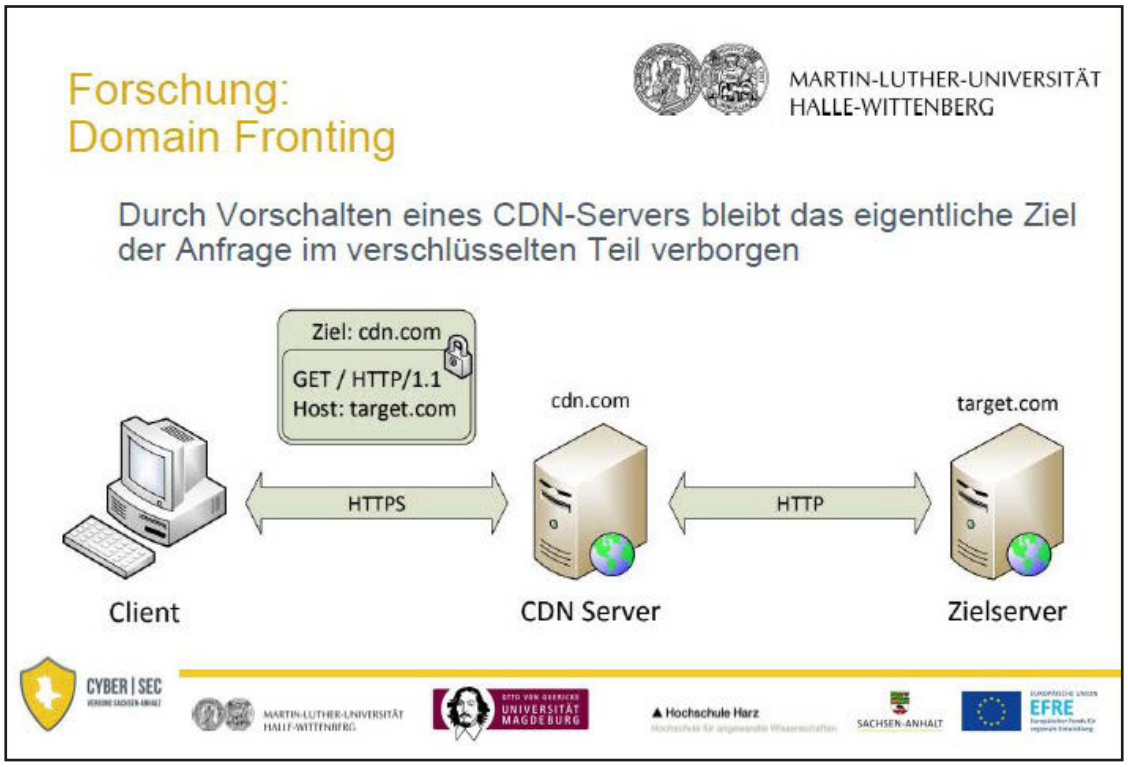
CYBER | SEC

▲ Hochschule Harz

SACHSEN-ANHALT

EFRE


Forschung:
Anwendung Kryptographie
MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG
Wie kann man Übertragungen trotz Verschlüsselung absichern?
IDS / Firewall
?
Angreifer können Verschlüsselung nutzen, um Sicherheitssysteme zu umgehen!
Client
SSL / TLS
SSH
Server
CYBER | SEC
Hochschule Harz
SACHSEN-ANHALT
EFRE


Forschung:
Domain Fronting
MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG
Durch Vorschalten eines CDN-Servers bleibt das eigentliche Ziel der Anfrage im verschlüsselten Teil verborgen
Ziel: cdn.com
GET / HTTP/1.1
Host: target.com
cdn.com
target.com
HTTPS
HTTP
Client
CDN Server
Zielserver
CYBER | SEC
Hochschule Harz
SACHSEN-ANHALT
EFRE

Lehre

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

Master Informatik

- Modul IT-Sicherheit
- Modul Praxis der IT-Sicherheit

Bachelor Informatik, Wirtschaftsinformatik, ...

- Modul Rechnernetze

Hörer aller Fakultäten

- Modul IT-Sicherheit

Grundlagen zum sicherheitsbewussten Umgang mit IT-Systemen, Erkennung und Vermeidung von Angriffsflächen

CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

Perspektiven

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

CyberSec-LSA OvGU

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Arbeitsgruppe Advanced Multimedia and Security Lab

(Otto-von Guericke-Universität Magdeburg, Pro. Dr. Dittmann):

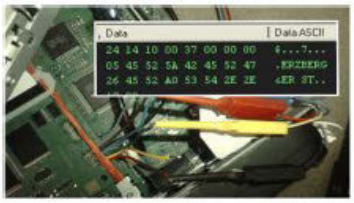
- Benutzerbiometrie und Interaktion
- Tatortforensik
- Daten- und Komponentenschutz
- Sicherheits-Benchmarks
- Evaluationsmethodiken
- Sicherheitsentwurfsmuster

AMSL
Advanced Multimedia and Security Lab

CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

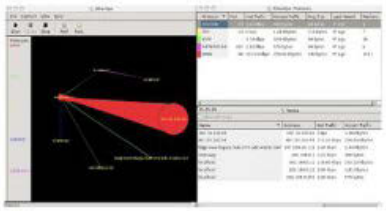
CyberSec-LSA OvGU

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG



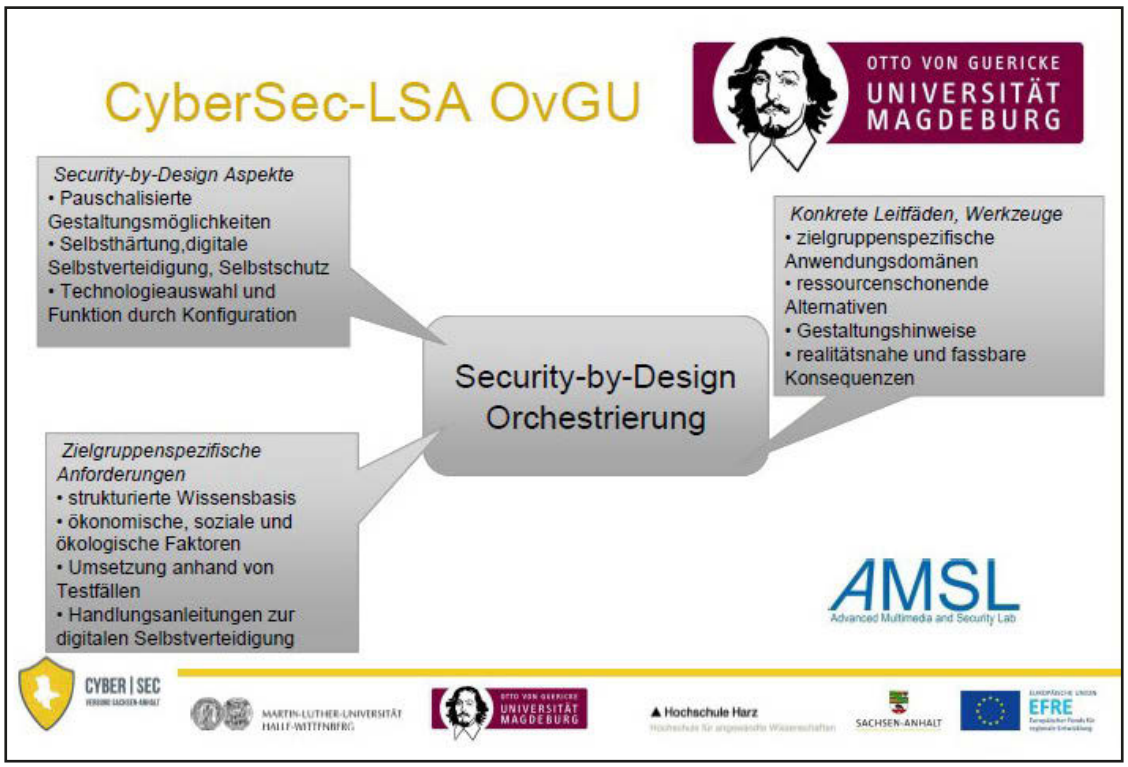
z. B. Forensik in
eingebetteten Systemen
(u.a. Automotive Forensik)

z. B. Forensik in
Desktop Systemen
(u.a. Netzwerkforensik)



Profilstudium ForensikDesign@Informatik

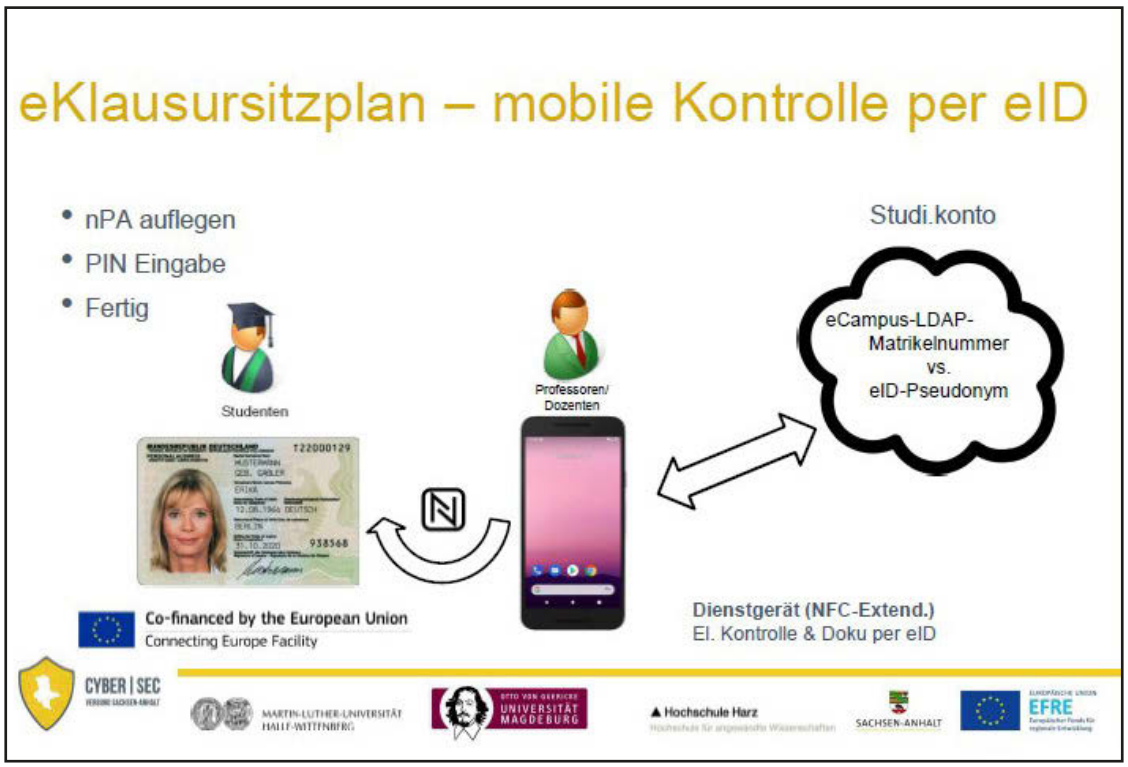
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE


CyberSec-LSA OvGU
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Security-by-Design Aspekte
• Pauschalisierte Gestaltungsmöglichkeiten
• Selbsthärtung,digitale Selbstverteidigung, Selbstschutz
• Technologieauswahl und Funktion durch Konfiguration
Konkrete Leitfäden, Werkzeuge
• zielgruppenspezifische Anwendungsdomänen
• ressourcenschonende Alternativen
• Gestaltungshinweise
• realitätsnahe und fassbare Konsequenzen
Security-by-Design Orchestrierung
Zielgruppenspezifische Anforderungen
• strukturierte Wissensbasis
• ökonomische, soziale und ökologische Faktoren
• Umsetzung anhand von Testfällen
• Handlungsanleitungen zur digitalen Selbstverteidigung
AMSL
Advanced Multimedia and Security Lab
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

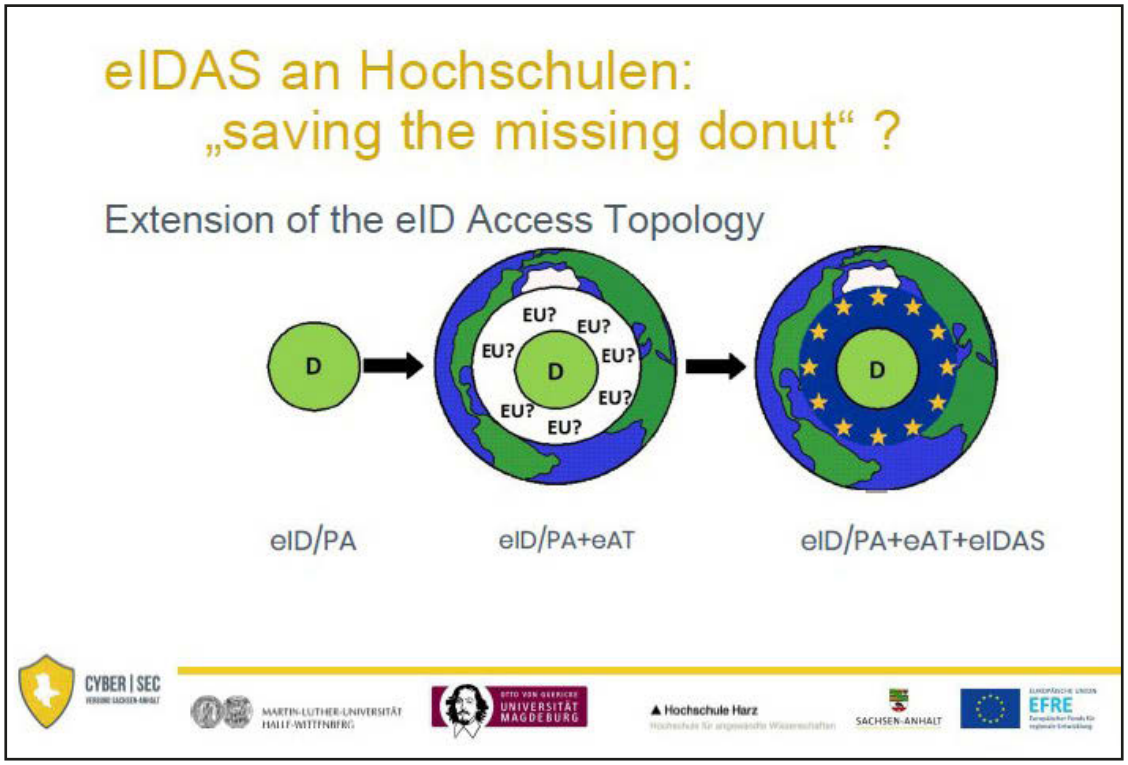

Schul- und Schülerwettbewerb:
• KOMPASS - Digitalisierung aber sicher!
• Entdecke Souveränität und Nachhaltigkeit
Thematik:
• Digitale Souveränität und digitale Nachhaltigkeit entdecken
• Souverän und nachhaltig denken und gestalten
• Schützen und sicher Agieren
• Analysieren und Reflektieren
• Security trifft Nachhaltigkeit
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

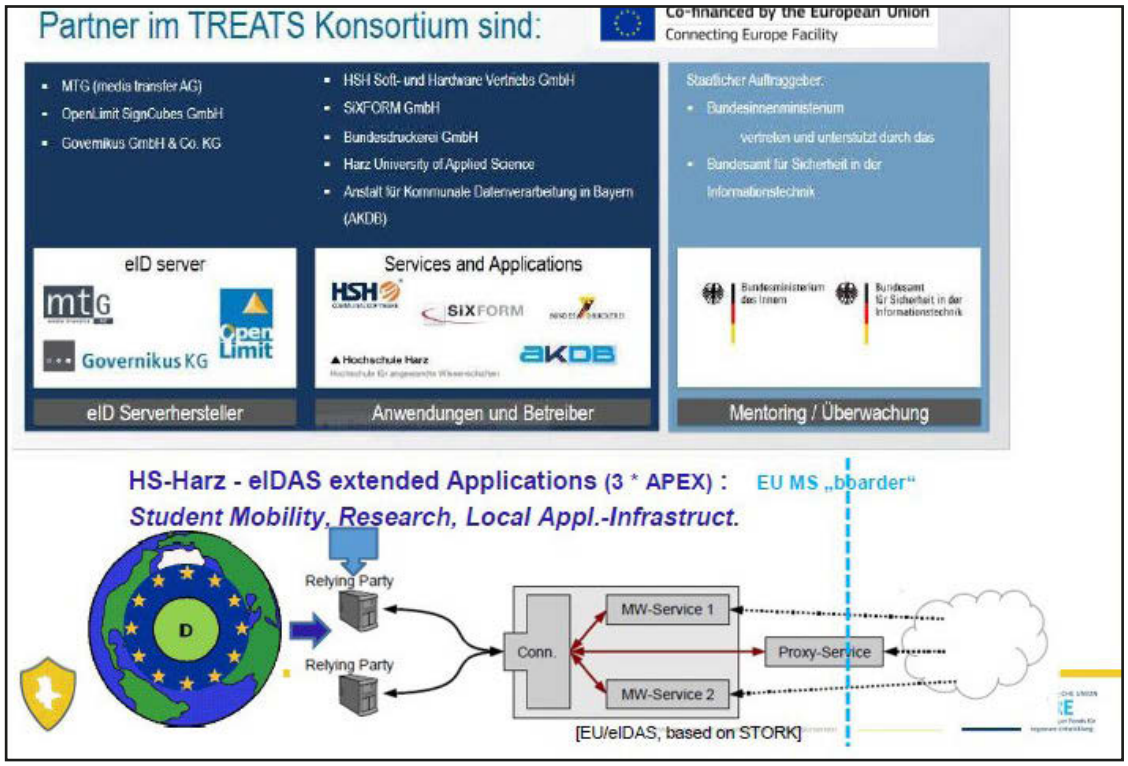

Schul- und Schülerwettbewerb:
Für wen?
• für Sachsen Anhalt
• für Schüler*innen sowie Lehrerschaft: Klassen/Gruppen aus Schulen oder
• Einzelpersonen (Schüler*innen, Lehrer*innen) sowie außerschulische Jugend- und Medienarbeit
• Werke von Kindern/Jugendlichen/ einschl. Lehrerschaft/Medien- und Sozialpädagog*innen ab
• Klasse 3 bis Klasse 12 und Berufsschüler aus Sachsen Anhalt
Einreichung bis zum 11.2.2020 bewerben
• Bewerbungen per email an sec-by-design@iti.cs.uni-magdeburg.de
• Preis: 3 Preisen zu je 3000 EURO und
• 20 KOMPASS-Mitmachworkshop an der OVGU oder in der Schule
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

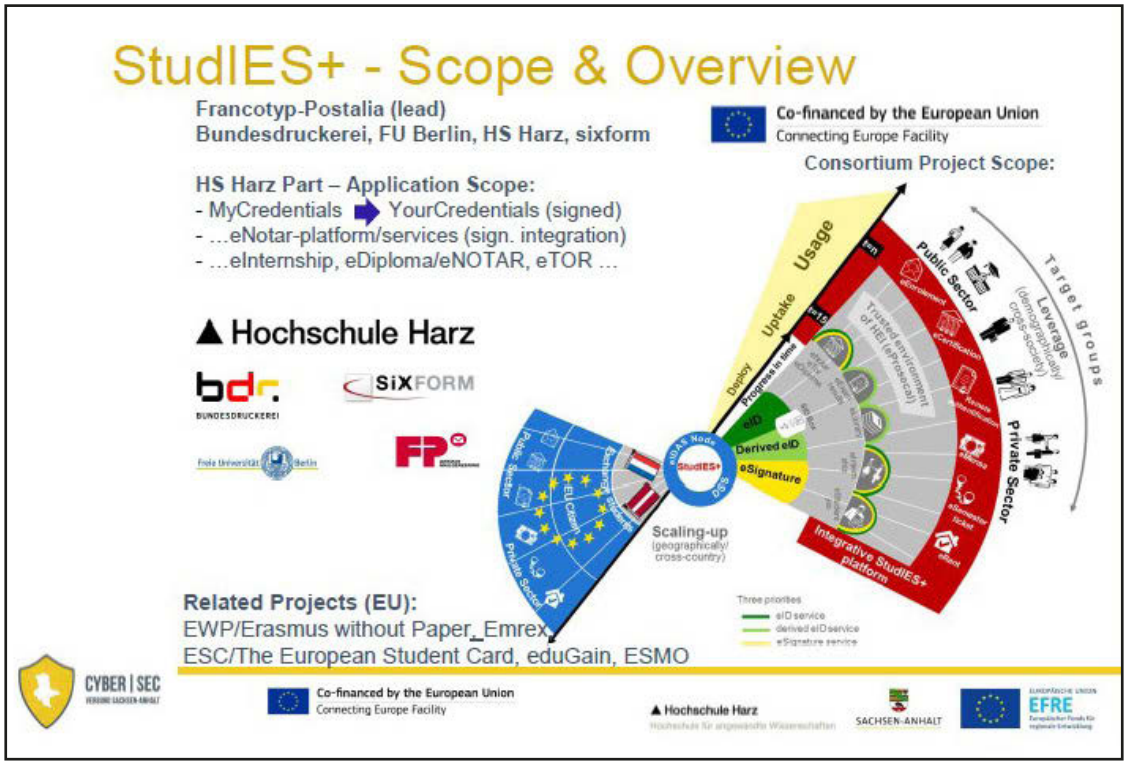

CyberSec-LSA: F&E-Vorarbeiten & Aktuelles
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE

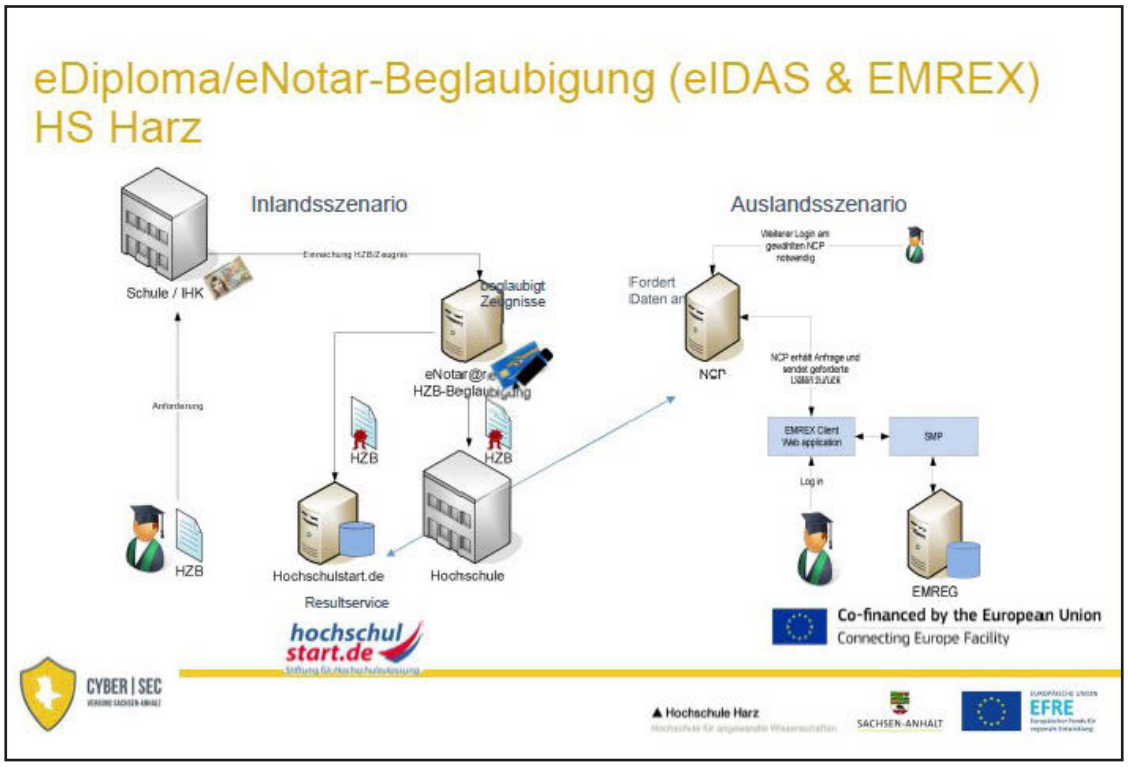

eKlausursitzplan – mobile Kontrolle per eID
nPA auflegen
PIN Eingabe
Fertig
Studi.konto
eCampus-LDAP-
Matrikelnummer
vs.
eID-Pseudonym
Studenten
Professoren/
Dozenten
Co-financed by the European Union
Connecting Europe Facility
Dienstgerät (NFC-Extend.)
El. Kontrolle & Doku per eID
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG
UNIVERSITÄT
MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE


EU TREATS/eIDAS-Workshop Berlin/LV LSA
Security-Workshop zur Digitalen Agenda LSA
Connecting Europe Facility
TREATS (TRans-European AuThentication Services)
Workshop
eIDAS-Erweiterungen für
eID-Szenarien
8. Juni 2017
Vertretung des Landes Sachsen-Anhalt beim Bund
Luisenstraße 16
10117 Berlin
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG
UNIVERSITÄT
MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE


eIDAS an Hochschulen:
„saving the missing donut“ ?
Extension of the eID Access Topology
D
EU?
EU?
EU?
EU?
EU?
EU?
EU?
D
D
eID/PA
eID/PA+eAT
eID/PA+eAT+eIDAS
CYBER | SEC
MARTIN-LUTHER-UNIVERSITÄT HALLE-WITTENBERG
UNIVERSITÄT MAGDEBURG
Hochschule Harz
SACHSEN-ANHALT
EFRE


Partner im TREATS Konsortium sind:
Co-financed by the European Union
Connecting Europe Facility
MTG (media transfer AG)
OpenLimit SignCubes GmbH
Governikus GmbH & Co. KG
HSH Soft- und Hardware Vertriebs GmbH
SIXFORM GmbH
Bundesdruckerei GmbH
Harz University of Applied Science
Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)
Staatlicher Auftraggeber:
Bundesinnenministerium
vertreten und unterstützt durch das
Bundesamt für Sicherheit in der Informationstechnik
eID server
Services and Applications
Bundesministerium des Innern
Bundesamt für Sicherheit in der Informationstechnik
eID Serverhersteller
Anwendungen und Betreiber
Mentoring / Überwachung
HS-Harz - eIDAS extended Applications (3 * APEX) :
EU MS „bborder“
Student Mobility, Research, Local Appl.-Infrastruct.
D
Relying Party
Relying Party
Conn.
MW-Service 1
Proxy-Service
MW-Service 2
[EU/eIDAS; based on STORK]


StudIES+ - Scope & Overview
Francotyp-Postalia (lead)
Bundesdruckerei, FU Berlin, HS Harz, sixform
Co-financed by the European Union
Connecting Europe Facility
Consortium Project Scope:
HS Harz Part – Application Scope:
- MyCredentials YourCredentials (signed)
- ...eNotar-platform/services (sign. integration)
- ...eInternship, eDiploma/eNOTAR, eTOR ...
Hochschule Harz
SiXFORM
Usage
Uptake
Deploy
Progress in time
Public Sector
Private Sector
Target groups
Leverage
(geographically/ cross-society)
eID
Derived eID
eSignature
StudIES+
Scaling-up
(geographically/ cross-country)
Integrative StudIES+ platform
Related Projects (EU):
EWP/Erasmus without Paper, Emrex,
ESC/The European Student Card, eduGain, ESMO
CYBER | SEC
Co-financed by the European Union
Connecting Europe Facility
Hochschule Harz
SACHSEN-ANHALT
EFRE


eDiploma/eNotar-Beglaubigung (eIDAS & EMREX)
HS Harz
Inlandsszenario
Auslandsszenario
Schule / IHK
beglaubigt
Zeugnisse
eNotar@
HZB-Beglaubigung
HZB
HZB
HZB
Hochschulstart.de
Resultservice
Hochschule
NCP
EMREX Client
Web application
SMP
EMREG
hochschul
start.de
Co-financed by the European Union
Connecting Europe Facility
CYBER | SEC
Hochschule Harz
SACHSEN-ANHALT
EFRE


Hochschule Harz
Hochschule für angewandte Wissenschaften
Harz University of Applied Sciences
MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG
OTTO VON GUERICKE
UNIVERSITÄT
MAGDEBURG
Security als Wirtschaftszweig /
Unterstützung durch Security-F&E
CYBER | SEC
SACHSEN-ANHALT
EFRE


Security als Wirtschaftszweig / Fazit 1
• Antrags- & Konzept-Beratung für Wirtschaft 4.0 / Digitalisierung / Förderung
• Security- und IT-IST-Aufnahmen/Tests, Security-Management & Policies
• Digitalisierung Produkte: Security by Design – Beratung, Prototyping, Tests
• verstärkte IT-Architekturen: vertrauenswürdige Security-Komponenten (Zertif.)
• Entwicklung: Sicherheits-Produkte & –Dienstleistungen, mit Security-Branding (LSA, D, EU), neue Möglichkeiten auch für KMU, via Security-Integrationen: z.B. per eIDAS (EU), PA- und Vertrauensdienste-Gesetze (D)
• Kooperation mit Unternehmen/Verbänden angestrebt
CYBER | SEC
SACHSEN-ANHALT
EFRE

Security als Wirtschaftszweig / Fazit 2

- Sicherheit in Bildung, Lehre, Fort-/Weiterbildung, Transfer (z.B. eID/eIDAS, eBeglaubig., Datenschutz-Kompass, Kryptoapplikat.)
- Security-F&E, auf wissl. Basis, mit Fach-Laboren & Fach-Personal, nachhaltig, kundennah
- Security als integraler Kern für Mehrwerte Wirtschaft 4.0 (Wirtschaftsförderung 5.0), Teil der Digitalen Agenda LSA
- Benchmarking - was machen Andere: s. FHG SIT Hessen (… ca. >= 200 MA & Mio. Förderungen)

CYBER | SEC · Martin-Luther-Universität Halle-Wittenberg · Otto von Guericke Universität Magdeburg · Hochschule Harz · Sachsen-Anhalt · EFRE

Fragen, Kontakte, F&E-Kooperationen

Prof. Dr. H. Strack

- Hochschule Harz, FB AI, netlab
  Friedrichstr. 57-59
  38855 Wernigerode
- Tel: +49 3943 659 341
- Mail: hstrack@hs-harz.de
- http://netlab.hs-harz.de/research/

Dr. S. Wefel

- Martin-Luther-Universität
  Halle-Wittenberg
  Institut für Informatik
  Von-Seckendorff-Pl. 1
  06120 Halle (Saale)
- Tel: +49 345 5524725
- Mail: sandro.wefel@informatik.uni-halle.de
- https://www.informatik.uni-halle.de/ti/

S. Kiltz

- Otto-von-Guericke-Universität
  Fakultät für Informatik
  Universitätsplatz 2
  39102 Magdeburg
- Tel: +49 391 6752838
- Mail: Kiltz@iti.cs.uni-magdeburg.de
- https://omen.cs.uni-magdeburg.de/itiamsl/home/index.html

CYBER | SEC · Martin-Luther-Universität Halle-Wittenberg · Otto von Guericke Universität Magdeburg · Hochschule Harz · Sachsen-Anhalt · EFRE

Schlusswort

Dr. Hilmar Steffen

Stellvertretender Leiter der Abteilung Verfassungsschutz im Ministerium für Inneres und Sport des Landes Sachsen-Anhalt

Es gilt das gesprochene Wort!

Sehr geehrte Damen und Herren,

der 3. Wirtschaftsschutztag neigt sich dem Ende zu. Mir obliegt es nun, Ihnen eine kurze Zusammenfassung zu geben.

Sie werden sicherlich bestätigen können, dass Informationen nur dem schaden, der sie nicht hat. Im Fall eigener Betroffenheit können Sie nicht sofort erkennen, ob Sie von einem fremden Nachrichtendienst oder Ihrer Konkurrenz angegriffen worden sind. Zur vertraulichen Bearbeitung steht Ihnen daher der Wirtschaftsschutz in Bund und Ländern auch nach der Veranstaltung zur Verfügung.

Ich hoffe, dass Sie heute nach Hause fahren in dem Bewusstsein, neue Aspekte und Möglichkeiten, vielleicht auch neue Gefahren für Ihr Unternehmen, Ihr Institut oder Ihre Behörde erkannt zu haben. Gleichzeitig gehe ich davon aus, dass Ihnen auch Lösungsansätze vorgestellt worden sind, die praktikabel sind und zu Ihrem Unternehmen passen.

Mit der Sensibilisierung von Management und Beschäftigten werden Sie für zukünftige Herausforderungen besser gewappnet sein und die spätere Kontaktaufnahme zum Wirtschaftsschutz steht Ihnen frei.

An dieser Stelle möchte ich der IHK Magdeburg für die gute und umfassende Zusammenarbeit und die Stellung der Räumlichkeiten danken. Des Weiteren danke ich meinen Kollegen aus dem Referat 44 für Ihr Engagement bei der Vorbereitung des 3. Wirtschaftsschutztages Sachsen-Anhalt.

Ich wünsche Ihnen allen einen guten Heimweg und hoffe, dass wir uns beim 4. Wirtschaftsschutztag 2021 in Halle (Saale) wiedersehen.


IHK MAGDEBURG
SACHSEN-ANHALT
Herzlich willkommen
zum
3. Wirtschaftsschutztag
des Landes Sachsen-Anhalt
“Neue Risiken, neue Bedrohungen?“


FREIHEITLICHE
DEMOKRATISCHE
GRUNDORDNUNG

Auf dem YouTube-Kanal der IHK Magdeburg finden Sie zudem ein kurzes Video mit weiteren Eindrücken des 3. Wirtschaftsschutztags: https://www.youtube.com/watch?v=EXbBg809E6Q.

Informationsblatt

„Wirtschaftsschutz in Sachsen-Anhalt“

Tagungsdokumentation

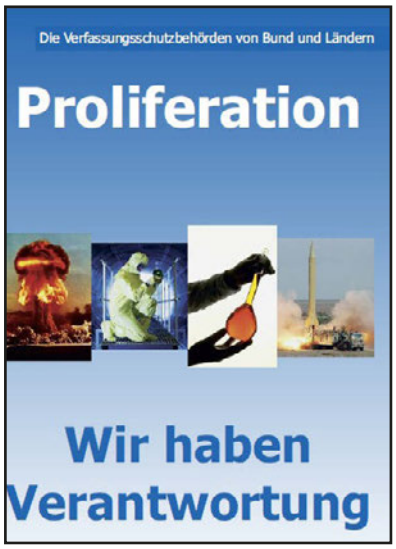
„Wirtschaftsschutztag Sachsen-Anhalt – Effizienter Schutz für Unternehmen im In- und Ausland“

Wirtschaftsschutztag am 16. September 2015 in Barleben

Tagungsdokumentation

2. Wirtschaftsschutztag Sachsen-Anhalt „Gut geschützt ist schwer gehackt“

Wirtschaftsschutztag am 25. Oktober 2017 in Halle (Saale)



Broschüre

Proliferation
„Wir haben Verantwortung“

Gemeinsame Broschüre des Bundesamtes für Verfassungsschutz und der Verfassungsschutzbehörden der Länder

Gemeinsame Informationsblätter des Bundesamtes für Verfassungsschutz und der Verfassungsschutzbehörden der Länder:

Unsere Themen.

Das sollten Sie wissen.

Cloud Computing. Was KMU wissen und beachten sollten.

Fokus Wissenschaft. Gefahren für Forschung und Lehre.

Industrie 4.0. Herausforderungen neuer Technologien.

Know-how-Schutz. Identifizieren. Bewerten. Schützen.

Geschäftsreisen. Sicherheit bei Auslandsreisen.

Besuchermanagement. Umgang mit Besuchern und Fremdpersonal.

Personalauswahl. Loyalität als Sicherheitsgewinn.

Sicherheitslücke Mensch. Gefahr durch Innentäter.

Social Media. Risiken durch soziale Netzwerke.

Verfassungsschutzbericht

Jährlicher Bericht des Verfassungsschutes über seine Beobachtungen und Analysen

Informationsblatt

„Was macht der Verfassungsschutz?“

Broschüre

„Kennzeichen des Rechtsextremismus“
(2. Auflage)

Eine Broschüre, die einen Überblick über die gängisten Kennzeichen, Symbole, Codes und Rituale der rechtsextremistischen Szene gibt.

Impressum

Herausgeber:	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt Halberstädter Straße 2/am „Platz des 17. Juni“ 39112 Magdeburg
Redaktion:	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt Referat Extremismusprävention, Spionageabwehr, Wirtschaftsschutz Nachtweide 82 39124 Magdeburg Tel.: 0391 567 3900 E-Mail: verfassungsschutz@mi.sachsen-anhalt.de www.mi.sachsen-anhalt.de/verfassungsschutz
Druck:	Fachhochschule Polizei Sachsen-Anhalt Stabsbereich I – Wissenschaftlicher Dienst/Medien –
Fotos Umschlag:	ra2studio - stock.adobe.com
Bildnachweis:	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt (Seite 1, 74) Industrie- und Handelskammer Magdeburg (Seite 4, Seite 75, 76) Laurence Chaperon (Seite 6) AV-TEST GmbH Magdeburg (Seite 9, 10, 11, 16, 17, 19, 27, 28, 29, 33) www.dunebook.com (Seite 19) Apple (Seite 23) Wikipedia (Seite 23) Teleport Sachsen-Anhalt GmbH (Seite 40, 41) Bundesamt für Sicherheit in der Informationstechnik (Seite 50) Hochschule Harz (Seite 56) Hochschule Harz, Martin-Luther-Universität Halle/Wittenberg, Otto-von-Guericke-Universität Magdeburg (Seite 58, 64, 65, 66, 70)

Stand: Juli 2020