4. Wirtschaftsschutztag Sachsen-Anhalt

Cybergefahren und Cyberabwehr

IHK Industrie- und Handelskammer Halle-Dessau

SACHSEN-ANHALT
Ministerium für Inneres und Sport

#moderndenken

Vorwort

Dr. Tamara Zieschang

Ministerin für Inneres und Sport
des Landes Sachsen-Anhalt

Sehr geehrte Damen und Herren,

der 4. Wirtschaftsschutztag am 11. November 2021 widmete sich den Themen „Cybergefahren und Cyberabwehr".

Die Digitalisierung von Konferenzen, Besprechungen, Vorlesungen und Schulungen hat sich während der Corona-Pandemie sprunghaft entwickelt. Viele Akteure in Wirtschaft und Gesellschaft haben neue Arbeitszeitmodelle und flexible Veranstaltungsformen etabliert. Wir sind gut vorangekommen auf dem Weg zu einer digitalen Gesellschaft.

Wie bei allen Veränderungen gilt es, die Menschen auf dem Weg der zunehmenden Digitalisierung mitzunehmen. Für Unternehmen heißt es, in anstehenden und laufenden Veränderungs- und Modernisierungsprozessen ihre Beschäftigten einzubeziehen und mitzunehmen. Dies gilt gerade auch in Bezug auf erforderliche Sicherheitsmaßnahmen.

Die BITKOM-Studie 2021 berichtete von einer starken Zunahme betroffener Unternehmen von Diebstahl, Industriespionage oder Sabotage. Bei Unternehmen zwischen zehn und 99 Mitarbeitenden waren nach eigenen Angaben 88 Prozent betroffen und 12 Prozent schätzten sich als „vermutlich betroffen" ein. Der Branchenverband BITKOM bezifferte die entstandenen Schäden im Verlauf von zwölf Monaten auf die Summe von 223,5 Milliarden Euro, was einer Verdoppelung im Verhältnis zum Jahr 2019 entspricht. Dies waren jedoch nur die messbaren Schäden bei Unternehmen mit mehr als zehn Mitarbeitenden. Über das Dunkelfeld können allenfalls grobe Schätzungen vorgenommen werden. Zum Dunkelfeld gehören unbemerkt gestohlene Daten durch Innentäter, Hacker oder Cyberspionage. Die Urheber der Schäden können wir der Cyber- oder Wirtschaftskriminalität, aber auch der Cyberspionage fremder Nachrichtendienste zuordnen.

Wir nehmen diese Entwicklung der zunehmenden Schadenssummen mit Sorge zur Kenntnis. Es bedarf daher einer gemeinsamen Kraftanstrengung, eines Schulterschlusses der Sicherheitsbehörden mit der Wirtschaft, um diese Gefahren für die Wirtschaft einzugrenzen und zu minimieren.

Der Wirtschaftsschutz, der im Ministerium für Inneres und Sport verankert ist, hat die Aufgabe, im Zusammenhang mit der Spionageabwehr präventiv mit Information und Beratung genau an dieser Stelle zu unterstützen. Die Information und Sensibilisierung von Unternehmen in Bezug auf Spionageaktivitäten fremder Nachrichtendienste, deren Ziele und Methoden sowie zu Handlungsempfehlungen für Schutzmaßnahmen ist seine Kernaufgabe. Der 4. Wirtschaftsschutztag, dessen Vorträge und Präsentationen Sie in diesem Tagungsband

nachvollziehen können, ist eines seiner zahlreichen Informationsangebote.

Die Unternehmen Sachsen-Anhalts müssen sich vor ungewollten Informationsabflüssen durch Wirtschaftsspionage und Cyberkriminelle schützen, egal wie groß der Umsatz oder die Zahl der Mitarbeitenden ist. Nach dem Gesetz zum Schutz von Geschäftsgeheimnissen gilt ein Geschäftsgeheimnis nur als solches, wenn Maßnahmen zu seinem Schutz getroffen worden sind.

Das Know-how von Unternehmen steht im Visier fremder Nachrichtendienste und konkurrierender ausländischer Unternehmen. Gerade die kleineren Unternehmen, die über keine eigene Sicherheitsabteilung verfügen, laufen stets Gefahr, Opfer aller Arten von Cyberangriffen zu werden. Gerade fremde Nachrichtendienste können sich zudem auf eine Palette von Mitteln und Methoden und langjährige Spionageerfahrungen stützen, die bei der Erstellung unternehmerischer Schutzkonzepte möglicherweise nicht alle Berücksichtigung fanden. Angriffe fremder Nachrichtendienste werden erfahrungsgemäß von vielen Detektionssystemen oft nicht einmal wahrgenommen.

Daher bleibt die zentrale Frage: Wie gehen Unternehmen mit ihren strategischen Wissensschätzen um? Wie ausreichend sind ihre Schutzmaßnahmen?

Der Wirtschaftsschutz Sachsen-Anhalt als Teil der Verfassungsschutzbehörde im Ministerium für Inneres und Sport steht Unternehmen in Sachsen-Anhalt kostenfrei und unverbindlich zur Verfügung, um mit Ihnen gemeinsam mehr Sicherheit im Unternehmen zum Schutz vor Spionage und Einflussnahme fremder Nachrichtendienste zu bewirken. Er kann auf die Expertise und die Unterstützung des Verfassungsschutzverbundes und insbesondere des Bundesamtes für Verfassungsschutz zurückgreifen, das mit einem Vortrag auf dem 4. Wirtschaftsschutztag präsent war. Der Wirtschaftsschutz steht Unternehmen bei der Identifizierung und Bewertung von Unternehmensrisiken sowie für In-House-Schulungen von Management und Mitarbeitenden zur Verfügung.

Informationen schaden nur dem, der sie nicht hat.

Kommen Sie auf uns zu, kontaktieren Sie den Wirtschaftsschutz Sachsen-Anhalt. Wir unterstützen Sie gern.

Magdeburg, im Dezember 2022

Inhalt

Einführung
Jochen Hollmann
Leiter der Abteilung Verfassungsschutz
im Ministerium für Inneres und Sport des Landes Sachsen-Anhalt 8

Begrüßung
Jörg Schlichting
Inhaber, EWS „Die Schuhfabrik“ e. K. und Vizepräsident der IHK Halle-Dessau *9*

„Digitale Fitness:
IT-Sicherheit in Unternehmen als Mannschaftssport”
Prof. Dr. Martina Sasse
Lehrstuhl Human-Centred Security,
Ruhr-Universität Bochum 11

„Cybersicherheit in Sachsen-Anhalt - Ein Lagebild“
Dr. Hilmar Steffen
Stellv. Leiter Verfassungsschutzbehörde
des Landes Sachsen-Anhalt 22

„Wirtschaftsschutz im Zeichen der Pandemie“
Vortrag des Bundesamtes für Verfassungsschutz 25

„Wie sich Unternehmen mit fünf einfach umzusetzenden Maßnahmen gegen nahezu alle Cyber-Bedrohungen schützen können“
Manuel Bach
Bundesamt für Sicherheit in der Informationstechnik 26

Impressionen 48

Ausgewählte Publikationen des Verfassungsschutzes 51

Einführung

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

Die sachsen-anhaltische Verfassungsschutzbehörde veranstaltet in den Jahren mit ungerader Jahreszahl gemeinsam mit den Industrie- und Handelskammern (IHK) des Landes den Wirtschaftsschutztag Sachsen-Anhalt im Wechsel in Magdeburg und in Halle (Saale). Am 11. November 2021 fand der 4. Wirtschaftsschutztag gemeinsam mit der IHK Halle-Dessau in deren Räumen statt.

Die gemeinsame Veranstaltung war durch zwei Randbedingungen stark geprägt. Zum einen forderte die COVID-19-Pandemie Überlegungen zur Durchführbarkeit ein. Auf Grund der einzuhaltenden Abstände und der Fläche der Räumlichkeiten der IHK ergab sich eine maximale Anzahl der physisch Teilnehmenden, die enttäuschend niedrig gewesen wäre. Schnell war die Entscheidung getroffen, die Veranstaltung sowohl in Präsenz als auch virtuell durchzuführen. Das Geschehen im Ludwig-Wucherer-Saal der IHK wurde elektronisch sowohl in den großen Veranstaltungsraum im ServiceCenter als auch über das Internet an angemeldete Online-Teilnehmer übertragen. Der IHK Halle-Dessau gilt unser Dank, da diese den Einsatz moderner Übertragungstechnik ermöglicht hat.

Eine weitere Randbedingung, die Einfluss auf die Inhalte nehmen sollte, waren die im Laufe des Jahres 2021 bekannt gewordenen schweren Cyberangriffe gegen Unternehmen und Kommunen in Sachsen-Anhalt mittels Ransomware. Auch wenn diese zumeist kriminell motiviert sein dürften, müssen wir davon ausgehen, dass Angriffe, die vom Territorium der Russischen Föderation auf Ziele in der ganzen Welt erfolgen, von den russischen Nachrichtendiensten auf Grund der umfassenden und uneingeschränkten Überwachungsmöglichkeiten toleriert werden.

Der 4. Wirtschaftsschutztag widmete sich daher primär der Thematik „Cybergefahren und Cyberabwehr“. Übersetzt in Maßnahmen der Prävention bedeutete dies, sowohl technische als auch verhaltensbezogene Hinweise in den Blick zu nehmen.

Sehr erfreulich war, dass wir erneut die Unterstützung des Bundesamtes für Verfassungsschutz (BfV) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hatten.

Die vorliegende Tagungsdokumentation bietet in kompakter Form die Tagungsbeiträge zum Nachlesen. Bitte beachten Sie, dass die Beiträge der Referentin und der Referenten deren Auffassungen zum Ausdruck bringen.
Mit insgesamt 200 Teilnehmenden – in Präsenz und virtuell – war der 4. Wirtschaftsschutztag der bislang erfolgreichste. Dies ermutigt uns, den 5. Wirtschaftsschutztag im Herbst 2023 in Magdeburg in den Blick zu nehmen. Wir freuen uns darauf, auch Sie dann begrüßen zu können.
Ich wünsche Ihnen eine informative Lektüre und möchte abschließend noch darauf hinweisen, dass Sie weitere Informationen zur Unternehmenssicherheit auf unserer Interseite www.mi.sachsen-anhalt.de/verfassungsschutz finden.

Magdeburg, im November 2022

Begrüßung

Jörg Schlichting
Inhaber, EWS „Die Schuhfabrik“ e. K. und Vizepräsident der IHK Halle-Dessau

Es gilt das gesprochene Wort!

Sehr geehrte Frau Ministerin Zieschang,
sehr geehrte Damen und Herren,

jedes Jahr am 11.11. um 11:11 Uhr wird der Karneval eingeläutet. In manchen Karnevalshochburgen wird das Rathaus gestürmt und die normale Ordnung außer Kraft gesetzt. Doch manchmal braucht es dazu gar keinen Karneval. Auch Cyberangriffe können Unternehmen, Kommunen, Krankenhäuser oder Rechtsanwälte außer Gefecht setzen. Das ist dann weitaus weniger spaßig als ein von Narren besetztes Rathaus.

Meine sehr geehrten Damen und Herren, ein herzliches Willkommen zum vierten Wirtschaftsschutztag Sachsen-Anhalt hier in der IHK Halle-Dessau. „Abwehr von Cyberattacken“ ist das Motto des heutigen Tages. Cyber-Bedrohungen können jeden treffen und deshalb fragt sich wohl jeder hier im Saal: Habe ich genügend Vorkehrungen getroffen? Kann ich mehr machen? Was genau könnte das sein? Fragen, die im unternehmerischen Alltag oft unbeantwortet bleiben oder von tagesaktuellen Themen überlagert werden.

Laut einer Umfrage des IT-Branchenverbandes Bitkom sind im letzten Jahr neun von zehn Unternehmen in unterschiedlichsten Ausprägungen Opfer von Cyberkriminalität geworden. Der verursachte Schaden wird mit 223 Milliarden Euro beziffert. Das entspricht 6,5 Prozent unseres BIP in 2020, 6,5 Prozent unseres Bruttoinlandsproduktes!

Deshalb soll es heute darum gehen, zu sensibilisieren, dass wir in einer immer stärker vernetzten Welt unser Verhalten überdenken und anpassen müssen. Nicht zuletzt seit Corona erbringen immer mehr Mitarbeiter ihre Arbeitsleistung am heimischen Bildschirm. Digitale Tools in Verwaltung und Management unterstützen unternehmerische Prozesse, verzahnen sich sowohl untereinander als auch mit digitalen Steuerungsprozessen in der Produktion und in der Lagerhaltung.

Sicher, wir alle sind froh über diese Entwicklungen, erleichtern sie uns doch das Agieren und Bestehen in einem immer komplexeren Marktumfeld – aber wir müssen sie beherrschen!

Sich dabei auf die eigenen IT-Spezialisten oder Dienstleister zu verlassen, ist wichtig, aber eben nicht ausreichend. Cyber-Sicherheit muss Chefsache sein. Doch die Mitarbeiter müssen dabei mitgenommen werden. Was kann ich als Chef tun, damit dieses Thema in meinem Unternehmen von jedem ernst genommen wird?

Da bin ich sehr gespannt auf Ihren Vortrag, sehr geehrte Frau Prof. Sasse, ein herzliches Willkommen.

Welche Bedrohungen denkbar sind und wie ein IT-Sicherheitsprozess im Unternehmen installiert werden kann, werden wir vom Bundesamt für Verfassungsschutz sowie von Herrn Manuel Bach vom vom Bundesamt für Sicherheit in der Informationstechnik, Herrn Manuel Bach erfahren. Seien Sie uns ebenfalls herzlich willkommen.

Herr Jochen Hollmann, der Leiter der hiesigen Verfassungsschutzbehörde, wird uns einen Einblick in das Lagebild zur Cybersicherheit in Sachsen-Anhalt geben. Lieber Herr Hollmann, wir freuen uns darauf.

Ganz besonders freuen wir uns, dass heimische Unternehmer von ihrem täglichen Umgang mit dem Thema Datensicherheit berichten und uns dabei einen Einblick in ihren unternehmerischen Alltag gewähren. Herr Koschmieder, Herr Dögel, Herr Prof. Döring und Herr Oppenhorst, seien Sie uns herzlich willkommen!

Den meisten von Ihnen wird Herr Michael Götschenberg vom ARD-Hauptstadtstudio kein Unbekannter sein. Wir danken Ihnen, lieber Herr Götschenberg, dass Sie uns mit Ihrer Expertise in Sicherheitsfragen durch den heutigen Tag führen.

„Digitale Fitness:
IT-Sicherheit in Unternehmen als Mannschaftssport“

Prof. Dr. M. Angela Sasse
Lehrstuhl Human-Centred Security,
Ruhr-Universität Bochum &
BSI Beirat Digitaler Verbraucherschutz

Es gilt das gesprochene Wort!

Meine sehr verehrten Damen und Herren,

dieser Beitrag beschreibt einen neuen Ansatz zur Entwicklung einer aktiven, positiven IT-Sicherheitskultur in Unternehmen. Ziel ist es, Mitarbeitende einzubinden und die Entwicklung von sicheren Routinen (Verhalten) zu unterstützen.

In der akademischen IT-Sicherheitsliteratur und im Diskurs unter Praktikern – auch bei Veranstaltungen wie dieser – taucht immer wieder der Begriff “Schwachstelle Mensch” auf. Damit ist gemeint, dass Mitarbeitende Opfer von Angriffen werden, die letztendlich dem Unternehmen gelten, und/oder dass sie die IT-Sicherheitsregeln des Unternehmens nicht befolgen. Unternehmen versuchen dem mit “Security Awareness” oder “Security Training” gegenzusteuern - diese gibt es von vielen Anbietern. Unternehmen in Deutschland geben dafür jedes Jahr Milliarden aus. Aber die Effektivität solcher Maßnahmen wird fast nie geprüft. Mehrere akademische Studien kommen zu dem Schluss, dass diese Maßnahmen allein nicht zu Verhaltensänderungen führen und auch das IT-Sicherheitswissen der Mitarbeitenden nicht nachhaltig verbessern.

Der “Schwachstelle Mensch” Ansatz sieht die Mitarbeitenden als Problem und fehlendes IT-Sicherheitswissen und Motivation als Grund für das falsche Verhalten. Wenn Mitarbeitende Fehler machen, ist der Grund “Unwissen, Ignoranz, Nachlässigkeit, Apathie, Bockigkeit und Schabernack”. Wenn man diesen Geschichten zuhört, kommt man zu dem Schluss, unsere IT Sicherheit würde super funktionieren, wenn nur die Mitarbeitenden die Sicherheitsregeln befolgen würden. Aber wenn Mitarbeitende IT-Sicherheitsregeln nicht befolgen, ist dies in der Regel, weil sie unmögliche Aufgaben stellt: Gedächtnisleistungen, die nur professionelle Gedächtnisathleten leisten können (Passwörter), kein oder nur umständlicher Zugang zu Informationen, die Mitarbeitende für ihre Arbeit brauchen. In der Praxis erfahren Mitarbeitende immer wieder, dass sie zwischen IT-Sicherheit und Erfüllung ihrer Produktionsziele wählen müssen. In den meisten Unternehmen wird dies ignoriert oder toleriert, bis es zu einem Sicherheitsvorfall kommt. So wird die Umgehung von IT-Sicherheitsregeln zur Gewohnheit, und IT-Sicherheit selbst nicht mehr Ernst genommen.

Im ersten Schritt sollten Unternehmen also herausfinden, warum Mitarbeitende bestimmte

Regeln des Sicherheitsverhaltens nicht befolgen. Ist der Grund die Unvereinbarkeit von Sicherheitsverhalten und Produktionszielen, muss eine machbare und sichere Lösung entwickelt werden. Wenn dies nicht geschieht, helfen Awareness oder andere auf die Mitarbeitenden gerichteten Interventionen wie Posterkampagnen, spielerische Interventionen oder sogenanntes Schubsen [2] nicht, egal wie bunt und teuer sie sind.

Wenn Mitarbeitenden die mit ihrem Verhalten verbundenen möglichen Schäden nicht klar sind, kann eine gezielte Awarenesskampagne mit klaren Handlungsanweisungen sowie Erinnerungen an das richtige Verhalten sinnvoll sein. Aber Information allein reicht nicht. Menschen ändern ihr Verhalten nur, wenn sie zuversichtlich sind, dass sie es können. Diese sogenannte Selbstwirksamkeit [3] können Unternehmen durch gezielte Trainings-maßnahmen, in denen das Verhalten geprobt und Rückmeldung gegeben wird, stärken. Gerade beim Umgang mit neuen Techniken wie Verschlüsselung oder Datasharing sind kurze Trainings vor Ort sehr effektiv.

90% menschlichen Verhaltens am Arbeitsplatz sind Routinen - Verhalten, da automatisch abläuft. Bei der Einführung neuer Sicherheitsregeln sollten Unternehmen unbedingt darauf achten, was die Auslöser für das alte, unsichere Verhalten sind, und diese entfernen oder ersetzten. Jede Wiederholung verstärkt das alte, unsichere Verhalten und verhindert, dass das neue, sichere Verhalten Routine wird. Wenn ich z.B. will, dass nur noch verschlüsselte USB-Sticks im Firmenkontext verwendet werden, sollten alle anderen aus dem Verkehr gezogen werden. Mehr Informationen zu den Stufen, die Mitarbeiter bei einer Verhaltensänderung durchlaufen, und wie man sie unterstützen kann, finden sie hier [4]. In diesem Zusammenhang möchte ich auch erwähnen, dass viele Menschen aufgrund schlechter Erfahrungen („Verstehe ich nicht. Kann ich nicht. Kann ich nicht umsetzen.“) IT-Sicherheit und Awareness-Maßnahmen skeptisch gegenüberstehen und auf “Durchzug” schalten. Dazu hat die verbreitete Praxis beigetragen, die Durcharbeitung solcher „Trainings” zu verlangen, damit man beim Audit ein Häkchen machen kann, und nicht nachzufragen, ob Mitarbeiter das Training verstehen, hilfreich finden oder befolgen können. Ich plädiere deshalb für einen neuen Begriff, für einen neuen Ansatz, der Mitarbeitende einbezieht und bei der Verhaltensänderung unterstützt: digitale Fitness.

Zusammenfassend:
Sicherheit muss machbar sein - Nutzbarkeit ist kein Luxus. Wenn Unternehmensleitung, Mitarbeitende und Sicherheitsexperten auf Konfrontation gehen, freuen sich die Angreifer, denn solche Unternehmen sind leichte Beute. Unternehmen müssen ihre IT-Sicherheit zusammen mit den Mitarbeitenden gestalten und verbessern und Verhaltensänderungen realistisch planen und unterstützen.

Bibliografie:

[1] Safa N. S., Von Solms, R. & Furnell, S. Information security policy compliance model in organizations. Computers & Security, Volume 56, February 2016, Pages 70-82.

[2] Thaler R. & Sunstein C.: Nudge: Wie man kluge Entscheidungen anstößt. Ullstein 2010

[3] Dennert P : Selbstwirksamkeit im Unternehmen - Das Konzept der Selbstwirksamkeit von Albert Bandura auf den betrieblichen Kontext angewendet. GRIN Verlag 2008.

[4] Sasse M.A., Hielscher J., Friedauer J. , Menges U., Peiffer M. (2022): Warum ITSicherheit in Organisationen einen Neustart braucht. In: Bundesamt für Sicherheit in der Informationstechnik (Hg.): Cyber-Sicherheit ist Chefinnen- und Chefsache, Tagungsband zum 18. Deutschen IT-Sicherheitskongress 2022, ISBN 978-3-922746-84-3, SecuMedia-Verlag Gau-Algesheim 2022.

Digitale Fitness:
IT Sicherheit in Unternehmen als Mannschaftssport

M. ANGELA SASSE, RUHR-UNIVERSITÄT BOCHUM & BSI Beirat Digitaler Verbraucherschutz

Übersicht

1. Was ist eigentlich das Problem?
   - Machbarkeit
   - Verständlichkeit
   - Verhaltensänderung statt Wissensaufbau
2. Sicherheitstraining 2.0
   - Digitale Fitness schrittweise aufbauen
   - Mitarbeiter aktiv miteinbeziehen (Konkordanz und Kooperation)
   - Verhaltensänderung unterstützen: Selbstwirksamkeit, intentionales Vergessen, 'Schubsen'

Problem: wie Sicherheitsexperten über Nutzer denken

MENSCHLICH – WELTOFFEN – LEISTUNGSSTARK 3

RUHR UNIVERSITÄT BOCHUM RUB

Sicherheitsforscher über Nutzer

Ignorant

Nachlässig

Apathisch

Bockig

Schabernack

"the lack of information security awareness, ignorance, negligence, apathy, mischief, and resistance are the root of users' mistakes"

Safa N. S., Von Solms, R. & Furnell, S. Information security policy compliance model in organizations. *Computers & Security*, Volume 56, February 2016, Pages 70-82.

MENSCHLICH – WELTOFFEN – LEISTUNGSSTARK 4

RUHR UNIVERSITÄT BOCHUM RUB

Problem Sicherheit = *Mission Impossible*

"Never give an order that can't be obeyed"
General Douglas MacArthur 1880-1964

5

RUHR UNIVERSITÄT BOCHUM RUB

Problem: IT Sicherheit als Produktivitätskiller

- Komplexe und zeitaufwendige Sicherheitsmassnahmen vernichten *Zeit, Aufwerksamkeit, Bereitschaft zum Mitmachen*
- Beispiele: Passwörter, CAPTCHAs, Anti-Phishing "Training"

Photo von Robert Watson
Cambridge University Computer Lab

RUHR UNIVERSITÄT BOCHUM RUB

THE WALL STREET JOURNAL.

The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1-d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

By *Robert McMillan*
Aug. 7, 2017 12:41 p.m. ET

The man who wrote the book on password management has a confession to make: He blew it.

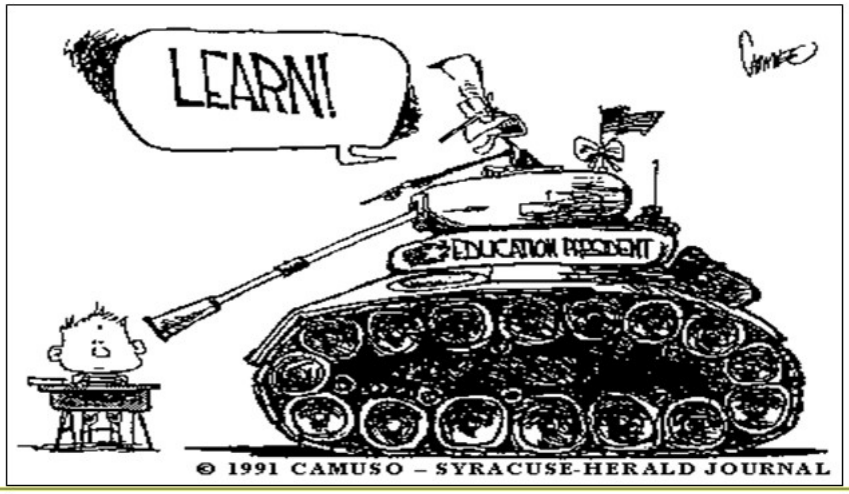
Der Vater von Nudging sagt ….

1. Schritt: Sicherheit ändern

Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

"Sicherheitsexperten können viel tun, um Mitarbeitern bei sicherem Verhalten zu unterstützen. Das kann durch Sicherheits-Training und Support-Funktion gehen, aber erfordert auch die Umstellung von Sicherheitspraktiken und –regeln, die mit den Produktszielen und Fähigkeiten der Mitarbeiter vereinbar sein müssen."

Schritt 2: Sicherheitstraining ändern



Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

"Interventionen, die den Glauben der Mitarbeiter an die eigene Fähigkeit ***(Selbstwirksamkeit)*** *richtigen Umgang mit Cyber-Bedrohungen stärken, führen eher zu Verhaltensänderungen als Kampagnen die nur die Bedrohung betonen."*

Weg mit Negativität und Furcht

- Securitsexperten versuchen Nutzer durch Furcht zu motivieren

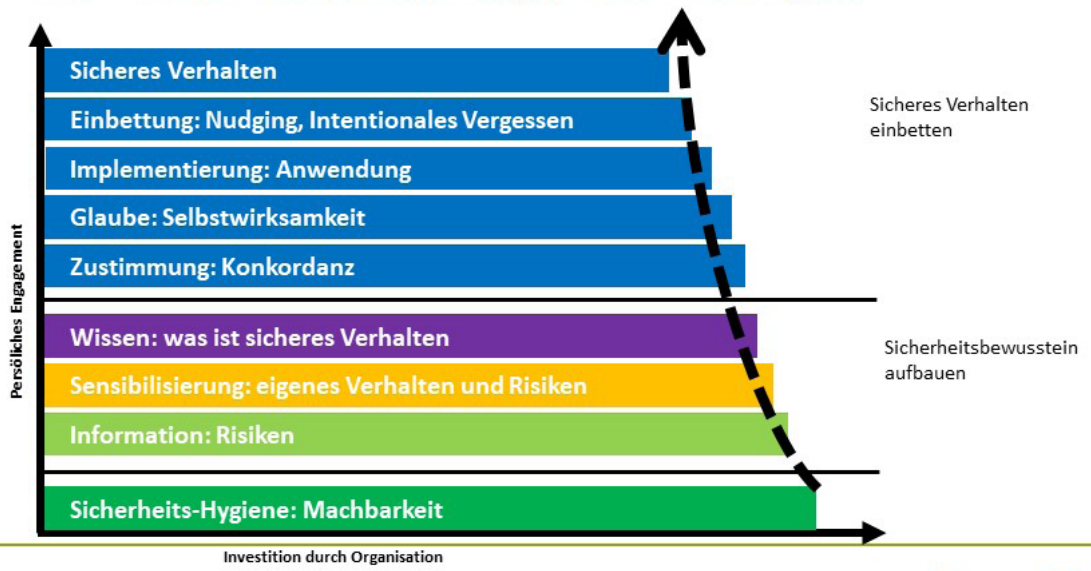
Another example: *Devil's in your details* https://www.youtube.com/watch?v=Ug18bmZF9Pc

12

Erfahrung von “Versagen“ = gelernte Hilflosigkeit

13

Die “Verhaltensänderungs-Kurve kriegen“



RUHR UNIVERSITÄT BOCHUM RUB

Wie verbessern wir IT Sicherheit?

1. Sicherheit muss machbar sein – Nutzbarkeit ist kein Luxus.
2. Wenn Nutzer und Sicherheitsexperten nicht zusammenarbeiten, freuen sich die Angreifer.
3. Zielsetzung und Gestaltung von Sicherheit mit, nicht gegen Nutzer.


USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It

ANNE ADAMS AND MARTINA ANGELA SASSE

In der Praxis …

1. Kommunikation
   - geteilte Verantwortung statt Verantwortung abschieben
   - respektvolle und positive Sprache
2. Sicherheitsmaßnahmen regelmässig evaluieren – und solche die nicht machbare und uneffizient sind, ausmisten.
3. Sicherheitsexperten müssen ansprechbar und hilfsbereit sein
4. Sicherheitsverhalten schrittweise umstellen, Prioritäten setzen, Erfolge feiern.

“Back to the future” – der ‘Kerkhoffs Test’ für IT Sicherheit

1. Das System muss im Wesentlichen (…) unentzifferbar sein.
2. Das System darf keine Geheimhaltung erfordern (…).
3. **Es muss leicht übermittelbar sein, und man muss sich die Schlüssel ohne schriftliche Aufzeichnung merken können (…).**
4. Das System sollte mit telegraphischer Kommunikation kompatibel sein.
5. **Das System muss transportabel sein und die Bedienung darf nicht mehr als eine Person erfordern.**
6. **Das System muss einfach zu benutzen sein, es darf keinen mentalen Stress verursachen oder das Merken eines Rattenschwanzes von Regeln erfordern.**

Auguste Kerckhoffs, ‘La cryptographie militaire’,
Journal des sciences militaires, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Feb. 1883.

17 Usable Security and Privacy: Human Factors

RUHR UNIVERSITÄT BOCHUM RUB

„Cybersicherheit in Sachsen-Anhalt - Ein Lagebild“

Dr. Hilmar Steffen

Stellv. Leiter Verfassungsschutzbehörde des Landes Sachsen-Anhalt

Es gilt das gesprochene Wort!

Sehr geehrte Frau Ministerin,

sehr geehrter Herr Vizepräsident Schlichting,

meine Damen und Herren,

auch ich darf Sie hier in den beiden Sälen in der IHK Halle-Dessau, an Ihren PCs und Endgeräten im Homeoffice oder im Büro herzlich begrüßen.

„Daten sind der Rohstoff des 21. Jahrhunderts.“ hat die amtierende Bundeskanzlerin Frau Dr. Angela Merkel erstmalig wohl im November 2015 geäußert.

Fakt ist, dass die Daten von Unternehmen, Behörden und Privatpersonen in einem bisher unbekannten Maß bedroht sind und zunehmend Daten durch Cyberangriffe verloren gehen.

Für die Abwehr und entsprechende Ermittlungen von Angriffen fremder Nachrichtendienste auf die IT-Netzwerke sachsen-anhaltischer Unternehmen, Behörden und Privatpersonen ist die Spionageabwehr zuständig. Diese kann sich insbesondere auf die vertrauensvolle Zusammenarbeit mit dem Bundesamt für Verfassungsschutz stützen. Da dem Verfassungsschutz keine exekutiven Befugnisse zustehen, bereitet die Verfassungsschutzbehörde die ihr vorliegenden Daten und Fakten auf. Sofern sich aus unserer Sicht ein Spionageverdacht ergeben sollte, werden die zuständigen Strafverfolgungsbehörden informiert, um Ermittlungen einzuleiten.

Bitte haben Sie Verständnis dafür, dass ich im Folgenden nicht einzelne betroffene Unternehmen oder Forschungseinrichtungen des Landes nenne, die in den Fokus von Cyber-Angreifern geraten sind.

Die Spionageabwehr arbeitet mit den Betroffenen auf vertrauensvoller und vertraulicher Basis zusammen, konkrete Vorfälle kommunizieren wir daher in aller Regel nicht in der Öffentlichkeit.

Allgemein schätzt die Spionageabwehr die Lage der Cyberspionage gegen Unternehmen und Institutionen im Land Sachsen-Anhalt wie folgt ein:

Cyberakteure fremder Nachrichtendienste haben auch sachsen-anhaltische Ziele im Blick. Es ist zu bedenken, dass Cyber-Angreifer ihre Attacken nicht als einzelnen Angriff durchführen. Sie greifen in der Regel nicht nur einzelne Ziele bzw. Unternehmen an und warten dann ab, ob sie ein Ergebnis erzielt haben und erfolgreich in ein Unternehmensnetzwerk

eingedrungen sind. Cyber-Angreifer führen ihre Attacken auch mit einer erfolgversprechenden Schadsoftware und einer größeren Menge an Zielen durch.

Die Schadsoftware ist sehr häufig aktuell und kann einen so genannten Zero-Day-Exploit (das ist eine bisher unbekannte, noch nicht dokumentierte Software-Schwachstelle) ausnutzen. Aber selbst wenn ältere Schadsoftware genutzt wird, kommt es vor, dass die in der Anti-Viren-Software eingebauten Mechanismen nicht anschlagen.

Folgende Ziele stehen im Fokus der Angreifer:

- Unternehmen und Behörden, die Kritische Infrastrukturen darstellen, wie z.B. Energieversorger oder Krankenhäuser,
- „Hidden Champions", das sind so genannte versteckte Weltmarktführer, z.B. kleine spezialisierte Unternehmen, die in Marktnischen sehr erfolgreich agieren,
- die beiden Universitäten des Landes,
- Unternehmen, die auch als Subunternehmer an Projekten des Bundes im Verteidigungssektor mitwirken,
- alle Unternehmen, die unter die „Made in China 2025"-Strategie fallen,
- Asylsuchende und Dissidenten aus autoritären Staaten und ihre Organisationen.

Für Cyberangriffe mit Zielen in Sachsen-Anhalt in den letzten zwölf Monaten zeichnen nach unseren Erkenntnissen die Nachrichtendienste folgender Staaten verantwortlich:

- die Russische Föderation,
- die Volksrepublik China und
- die Islamische Republik Iran.

Als potenzielle Angreifer werden weiterhin Nordkorea und die Türkei eingeschätzt. Je nach Interessenlage können Nachrichtendienste weiterer Staaten hinzukommen.

Staatliche bzw. halbstaatliche Cyberakteure der Russischen Föderation griffen zuletzt die Router zweier Unternehmen an, um die Konfigurationsdatei auszuleiten. Die Fülle dieser Dateien sollte weitere Angriffe und ein Eindringen in die jeweiligen IT-Netzwerke vorbereiten.

Im Dezember 2020 griffen Hacker den Downloadbereich der Firma Solarwinds an. Es gelang ihnen, die abrufbereite Netzwerküberwachungssoftware „Orion" mit Schadsoftware zu infizieren. Es wurden 18.000 Unternehmen weltweit angegriffen. Die Attacke wird dem russischen Auslandsnachrichtendienst SWR zugeschrieben.

Im März informierte das Software-Unternehmen Microsoft die Öffentlichkeit über drei kritische Schwachstellen in der Software „Microsoft Exchange Server". Der erste Hinweis darauf erfolgte bereits im Dezember 2020 und schon im Januar 2021 fanden erste Angriffe unter Ausnutzung dieser Exploits statt. Schon wenige Wochen nach Microsofts „Patchday" im März dieses Jahres mussten IT-Sicherheitsbehörden feststellen, dass mutmaßlich chinesische Hacker diese Schwachstellen für Cyberangriffe ausnutzten.

Die Botschaft ist also: ein schnelles „Patchen" kann Cyberangriffe unterbinden.

Auch Forschungseinrichtungen in Sachsen-Anhalt verzeichneten 2016 Angriffe. Das so genannte „Mabna-Institut" der iranischen Revolutionswächter (Pasdaran) hatte insgesamt 160 weitere Hochschuleinrichtungen und Universitäten weltweit angegriffen, um einen

Zugang zu den wissenschaftlichen Arbeiten zu erzwingen. Terabytes von Daten sollen Richtung Iran geflossen sein. Diese Angriffe setzten sich 2021 fort. Der Generalbundesanwalt ermittelt.

Die autoritären Staaten China, Russland, Nordkorea, Iran sind unter Ausnutzung von Software-Schwachstellen bemüht auch Ziele in Sachsen-Anhalt anzugreifen, um ihre unterschiedlichen Interessen zu verfolgen. Was die Zuordnung der Angriffe betrifft, muss festgehalten werden, dass das Internet einiger Staaten zunehmend bzw. ziemlich vollständig vom restlichen Internet abgeschottet ist und die Internetverkehre überwacht und ggf. zensiert werden. Deshalb müssen Angriffe, die über Server dieser Staaten geführt werden, von den dortigen Internet-Überwachungsorganisationen, wie Geheimdiensten, zumindest geduldet werden. Womöglich werden derartige Aktivitäten auch von staatlichen Stellen gefördert.

Weiterhin gibt es vereinzelte Fälle, in denen die Spionageabwehr / der Wirtschaftsschutz um Sensibilisierung der betreffenden Unternehmen gebeten wird. Diesen Bitten kommen wir gern nach.

Die Spionageabwehr ist zwar für kriminelle Cyberangriffe nicht zuständig, muss aber ihren zunehmend bedrohlichen Charakter für das Funktionieren unseres Gemeinwesens zur Kenntnis nehmen. Der Verbleib der geraubten und ins Internet hochgeladenen Daten bereitet uns Sorge, weil sie möglicherweise im „Darknet“ verkauft und von Nachrichtendiensten oder Kriminellen dort erworben werden können.

Die Lage der Cybersicherheit in Sachsen-Anhalt möchte ich wie folgt zusammenfassen:

- Fremde Nachrichtendienste verfolgen bevorzugt die Ausspähungsinteressen ihrer Länder. Unter Ausnutzung einer ganzen Palette von Angriffsvarianten sammeln sie illegal Daten zu Kritischen Infrastrukturen, Hidden Champions und Spitzentechnologien.

- Dabei gehen sie breit aufgefächert vor. Angriffe chinesischer, russischer und iranischer Cyberakteure gegen sachsen-anhaltische Unternehmen, Hochschulen und Behörden finden statt und können jederzeit fortgesetzt werden. Sie betreiben Wirtschaftsspionage.

- Es ist weiterhin mit Ransomware- und nachrichtendienstlichen Cyber-Angriffen zu rechnen.

Meine sehr verehrten Damen und Herren,

wir alle sind als Endanwender gefordert, uns um die Sicherheit der uns anvertrauten IT-Systeme zu kümmern. Was wir dabei zu tun haben, werden uns Vertreter vom Wirtschaftsschutz im BfV sowie Herr Bach als Vertreter des BSI näherbringen.

„Wirtschaftsschutz im Zeichen der Pandemie“

Vortrag des Bundesamtes für Verfassungsschutz

Es gilt das gesprochene Wort!

Der Vortrag des BfV unter dem Titel „Wirtschaftsschutz im Zeichen der Pandemie“ skizzierte den Arbeitsansatz des Präventionsbereichs der Behörde und stellte anhand verschiedener Fallbeispiele aus den dortigen Phänomenbereichen Implikationen der Pandemie für die Arbeitsbereiche des BfV dar.

So wurde exemplarisch die Sensibilisierung deutscher Unternehmen und Forschungseinrichtungen, die in Lieferketten der Impfstoffentwicklung und -Produktion eingebunden sind, vorgestellt. Hier waren mittels zielgerichteter Sicherheitshinweise über geeignete Kommunikationskanäle alle relevanten Akteure der Branche adressiert worden.

Auch staatliche Desinformationskampagnen gegen deutsche Forschungsinstitute und Unternehmen der Biotechnologie sowie Radikalisierungstendenzen im politischen Extremismus wurden dargestellt.

Das BfV war außerdem mit einem eigenen Stand beim Wirtschaftsschutztag vertreten.

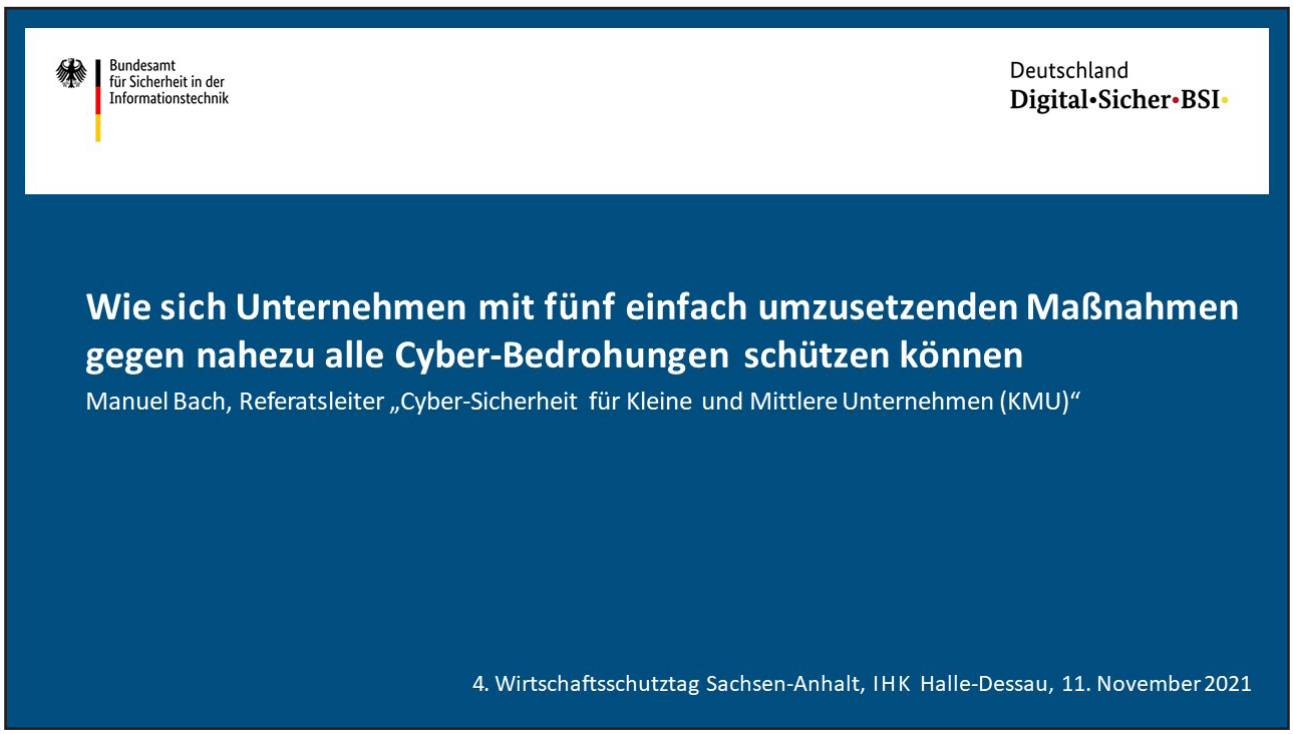
Anmerkung des Wirtschaftsschutzes Sachsen-Anhalt:

Der Wirtschaftsschutz des BfV war nicht zum ersten Mal mit einem Stand und reichlichem Informationsmaterial beim sachsen-anhaltischen Wirtschaftsschutztag vertreten. Bereits 2015 im IGZ Barleben (Bördekreis), 2017 in den Räumen der IHK Halle-Dessau in Halle (Saale) und 2019 in den Räumen der IHK Magdeburg in der Landeshauptstadt war der BfV-Stand ein greifbares Symbol der engen vertrauensvollen Zusammenarbeit. Am Stand des BfV trafen sich in den Pausen und beim Get-together jedes Mal Teilnehmende, Gäste, Referenten und Veranstalter zu spannenden Gesprächen und Diskussionen. Das Wirtschaftsschutzteam Sachsen-Anhalt dankt an dieser Stelle dem BfV für die stetige gute Zusammenarbeit und freut sich auf den BfV-Stand beim 5. Wirtschaftsschutztag 2023 in Magdeburg.

„Wie sich Unternehmen mit fünf einfach umzusetzenden Maßnahmen gegen nahezu alle Cyber-Bedrohungen schützen können“

Manuel Bach
Bundesamt für Sicherheit in der Informationstechnik

Es gilt das gesprochene Wort!



Wie bedroht ist Deutschlands Cyber-Raum?

- **Ausweitung** bekannter cyber-krimineller Erpressungsmethoden
- Neben **Lösegelderpressungen** traten **Schweigegelderpressung** unter Androhung der Enthüllung kompromittierender Informationen (Double Extortion) und **Schutzgelderpressungen** unter Androhung von DDoS auf.
- Rund **144 Mio. Variationen von neuen Schadprogrammen** wurden im Berichtszeitraum gesichtet. Das sind durchschnittlich **394.000 pro Tag, in Spitzenwerten 533.000 (höchster je gemessener Wert)**.
- **Rund 98 %** aller geprüften Systeme waren durch **Schwachstellen in Microsoft Exchange-Servern** verwundbar.
- Bei Angriffen auf die Bundesverwaltung wurden rund **44.000 E-Mails mit Schadsoftware pro Monat** abgefangen.
- **COVID-19-Pandemie**: Neue Gefährdungslage durch Cyber-Angriffe auf **Firmen und Behörden aus dem Gesundheitsbereich**

Quelle: BSI

Bundesamt für Sicherheit in der Informationstechnik

Seite 3

Quelle: BSI

Bundesamt für Sicherheit in d Informationstechnik

Seite 4

Bundesamt für Sicherheit in der Informationstechnik

Artikel 3:

„Et hätt noch emmer joot jejange.“*

- * … in einer anderen Zeit und unter völlig anderen Rahmenbedingungen!

Cyber-Sicherheit in der Digitalisierung

Vernetzung

Komplexität

Allgegen-wärtigkeit

Digitalisierung bedeutet…

…mehr Möglichkeiten,

auf die Deutschland nicht verzichten kann und soll

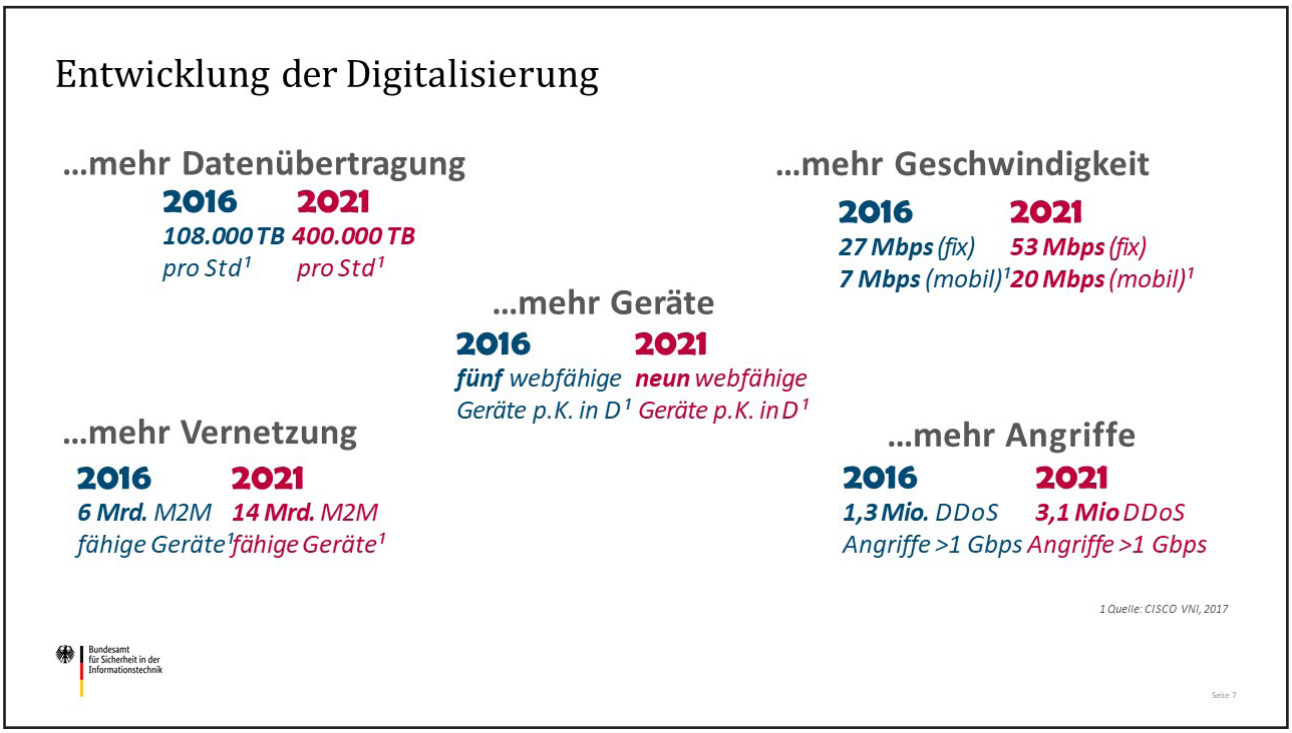
…mehr Gefahren,

auf die Deutschland vorbereitet sein muss

Cyber-Sicherheit **…unverzichtbare Voraussetzung für das Gelingen der Digitalisierung**

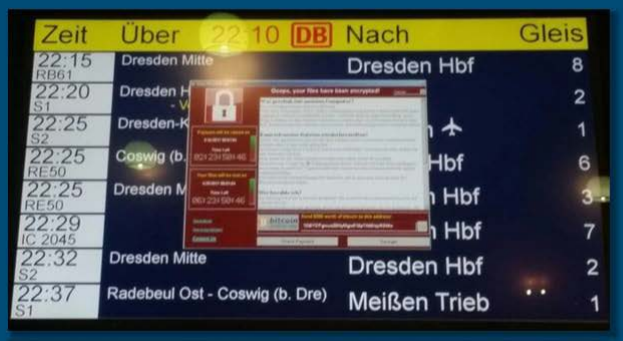
Bundesamt für Sicherheit in der Informationstechnik

Seite 6


Entwicklung der Digitalisierung
...mehr Datenübertragung
2016 2021
108.000 TB pro Std[1] 400.000 TB pro Std[1]
...mehr Geschwindigkeit
2016 2021
27 Mbps (fix) 53 Mbps (fix)
7 Mbps (mobil)[1] 20 Mbps (mobil)[1]
...mehr Geräte
2016 2021
fünf webfähige Geräte p.K. in D[1] neun webfähige Geräte p.K. in D[1]
...mehr Vernetzung
2016 2021
6 Mrd. M2M fähige Geräte[1] 14 Mrd. M2M fähige Geräte[1]
...mehr Angriffe
2016 2021
1,3 Mio. DDoS Angriffe >1 Gbps 3,1 Mio DDoS Angriffe >1 Gbps
1 Quelle: CISCO VNI, 2017
Bundesamt für Sicherheit in der Informationstechnik
Seite 7


Bundesamt für Sicherheit in der Informationstechnik
Ohne Cyber-Sicherheit keine erfolgreiche Digitalisierung!

Bundesamt
für Sicherheit in der
Informationstechnik



Bundesamt
für Sicherheit in der
Informationstechnik

„Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite“

„Garmin mit Komplettausfall“

„Angreifer legtenAlu-Konzern mit Erpressersoftware lahm“

„Hackerangriff auf Uniklinik: Ermittlungen wegen fahrlässiger Tötung eingeleitet“

Bundesamt
für Sicherheit in der
Informationstechnik


Deutschlandfunk

Datenschutz

Cyberangriff auf das Berliner Kammergericht

Nach einem Cyberangriff auf das Berliner Kammergericht ist bislang unklar, ob Daten abgeflossen sind. Die Hacker konnten womöglich auf alle Daten des Gerichts zugreifen, so der Präsident des Gerichts. Hackerangriffe werden für Behörden zunehmend zur Gefahr.

Von Johannes Kuhn

„Das Kammergericht ist eigentlich überall", so die Berliner IT-Staatssekretärin Sabine Smentek (Imago / Christian Ditsch)


heise online

Uni Gießen nähert sich nach Hacker-Attacke wieder dem Normalbetrieb

Aufgrund eines IT-Sicherheitsvorfalls war die Universität Gießen um Weihnachten 2019 zeitweise komplett offline. Nun gehen erste Dienste wieder online.

(Bild: dpa, Oliver Berg)

06.01.2020 14:19 Uhr

Bundesamt
für Sicherheit in der
Informationstechnik

Mögliche Cyberattacke: Stadt Potsdam nimmt Server der Verwaltung vom Netz

Nach Malware-Infektion: Katastrophenfall im Landkreis Anhalt-Bitterfeld

KEINE E-MAILS, FRANKFURT.DE OFFLINE

„Emotet" legt Stadt-Computer lahm

Stadtwerke Wismar: Ermittlungen nach Cyberattacke laufen

Hackerangriff auf Verwaltungen in Wesel und Witten

Brandenburg fährt die Server runter

CYBERANGRIFF

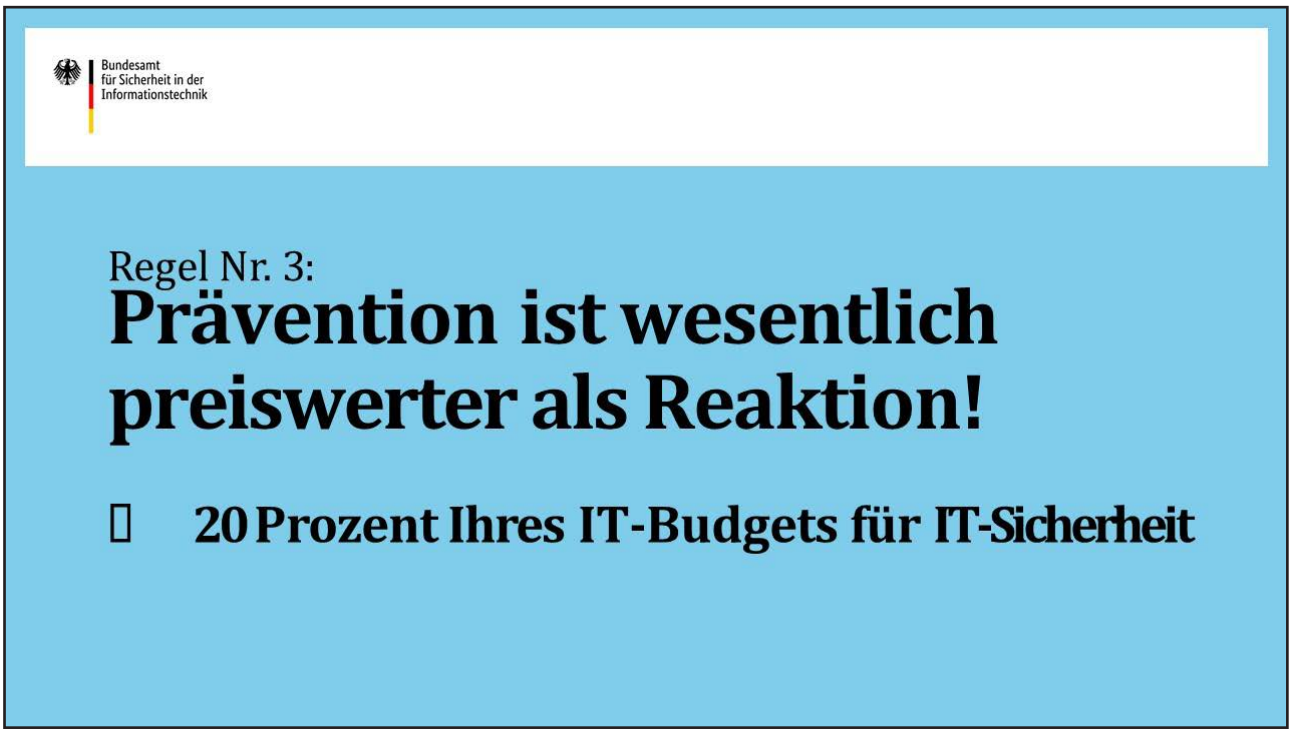
Hackerangriff in Mecklenburg-Vorpommern legt Kommunalverwaltungen seit Tagen lahm

SCHWERIN UND LUDWIGSLUST-PARCHIM

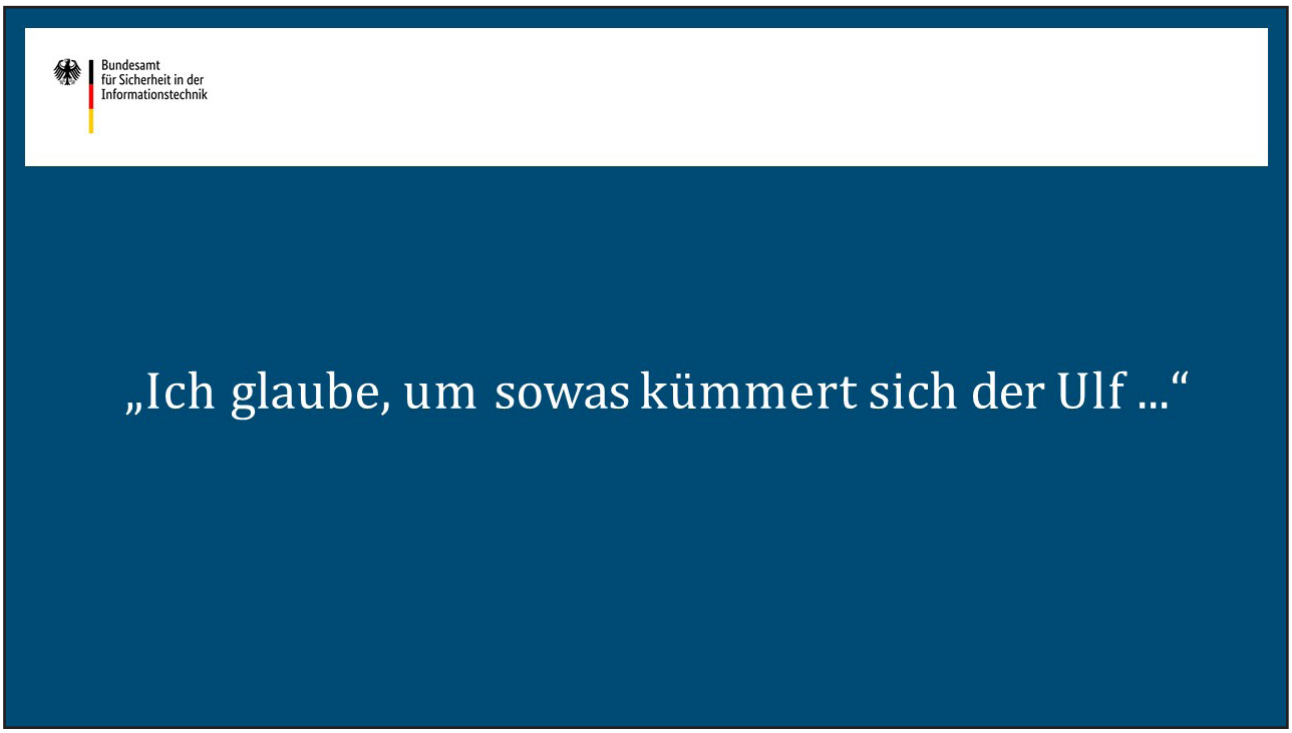
Probleme nach Cyberangriff dauern an – Sicherheitslücke bisher nicht gefunden


Bundesamt
für Sicherheit in der
Informationstechnik
Regel Nr. 1:
Jeder wird angegriffen -
Es gibt keine Ausnahmen!
Identifizieren Sie Risikoprofil u. Kronjuwelen
Sensibilisieren Sie Ihre Mitarbeiter
Sichern Sie Ihre Systeme möglichst gut ab


Bundesamt
für Sicherheit in der
Informationstechnik
Regel Nr. 2:
Früher oder später werden Ihre
Schutzmaßnahmen versagen!
Erarbeiten Sie ein Notfallkonzept
Befolgen Sie Ihre Backup-Strategie
Bereiten Sie die Einholung externer Hilfe vor
Schließen Sie ggf. eine Cyber-Versicherung ab


Bundesamt
für Sicherheit in der
Informationstechnik
Regel Nr. 3:
Prävention ist wesentlich preiswerter als Reaktion!
20 Prozent Ihres IT-Budgets für IT-Sicherheit


Bundesamt
für Sicherheit in der
Informationstechnik
Regel Nr. 4:
Teure Reaktion ist immer noch preiswerter als Kapitulation!
Professionelle externe Hilfe kann kostspielig sein, ist aber oftmals nötig


Bundesamt
für Sicherheit in der
Informationstechnik
„Ich glaube, um sowas kümmert sich der Ulf ...“


Bundesamt
für Sicherheit in der
Informationstechnik
IT-Sicherheit ist
Chefsache!

Bundesamt
für Sicherheit in der
Informationstechnik

Sorgen Sie für klare Zuständigkeiten!

Bundesamt
für Sicherheit in der
Informationstechnik

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

0800-ULF

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Bundesamt
für Sicherheit in der
Informationstechnik

Die 5G-Regel

- Gesichert
- Geupdated
- Geblockt
- Gehabt
- Geübt

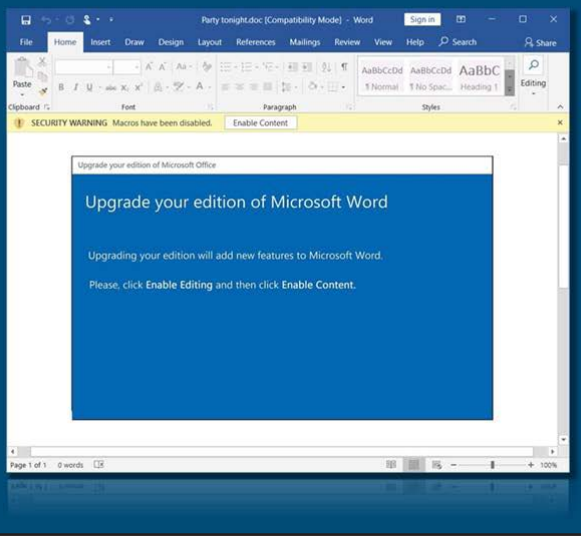
Bundesamt
für Sicherheit in der
Informationstechnik

#1
Backups bringen Beruhigung

Bundesamt
für Sicherheit in der
Informationstechnik

#2
Malware mag Makros!

Bundesamt
für Sicherheit in der
Informationstechnik



Typischer Angriff über Makros

Kostenlose Gegenmaßnahme

- Deaktivieren Sie in den Windows-Gruppenrichtlinien die Ausführung von Makros.
- Falls Makros unbedingt benötigt werden, lassen Sie nur signierte Makros zu.

Bundesamt
für Sicherheit in der
Informationstechnik

#3
Passwörter peinigen Planlose

Bundesamt
für Sicherheit in der
Informationstechnik

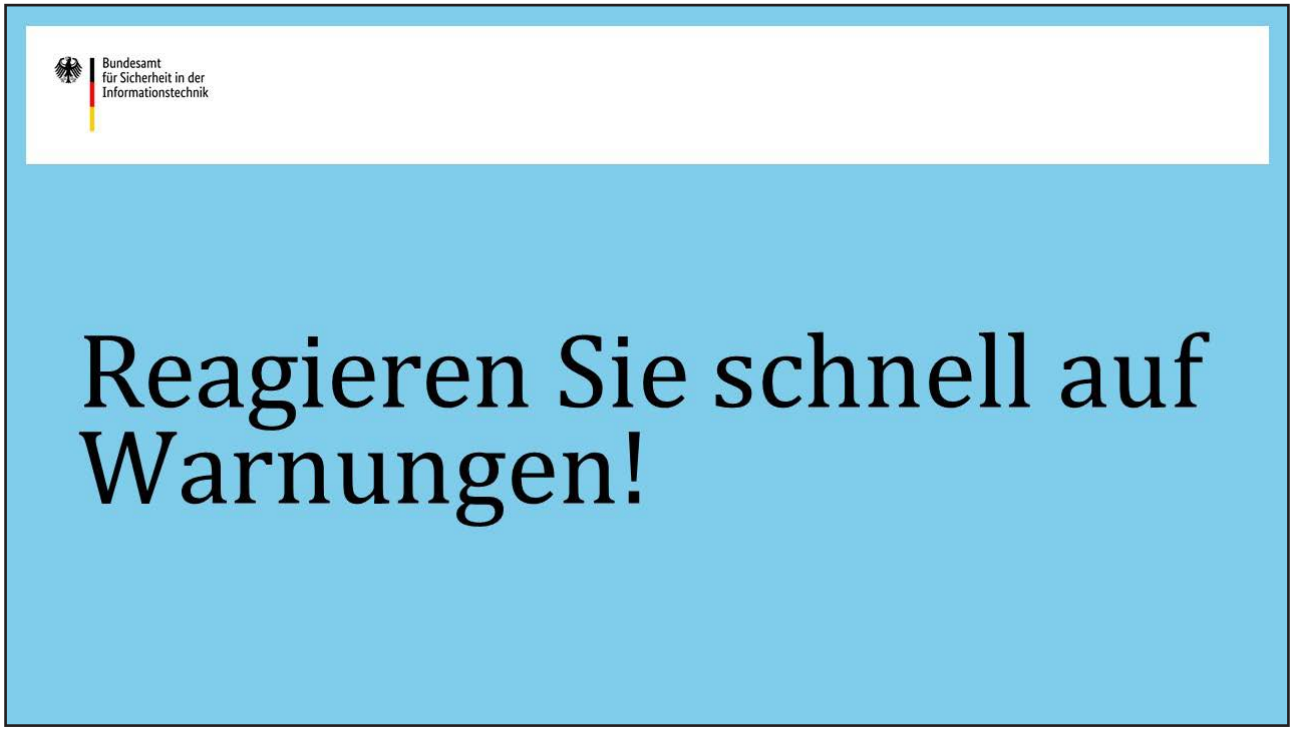
Typischer Phishing-Angriff

Gegenmaßnahmen

- Komplexe Passwörter
- Passwort-Manager
- Zwei-Faktor-Authentisierung

1. 123456
2. 123456789
3. 12345678
4. 1234567
5. Password
6. 111111
7. 1234567890
8. 123123
9. 000000
10. abc123


Bundesamt
für Sicherheit in der
Informationstechnik
#4
Updates umfahren
Untiefen


Bundesamt
für Sicherheit in der
Informationstechnik
Reagieren Sie schnell auf
Warnungen!

Bundesamt für Sicherheit in der Informationstechnik

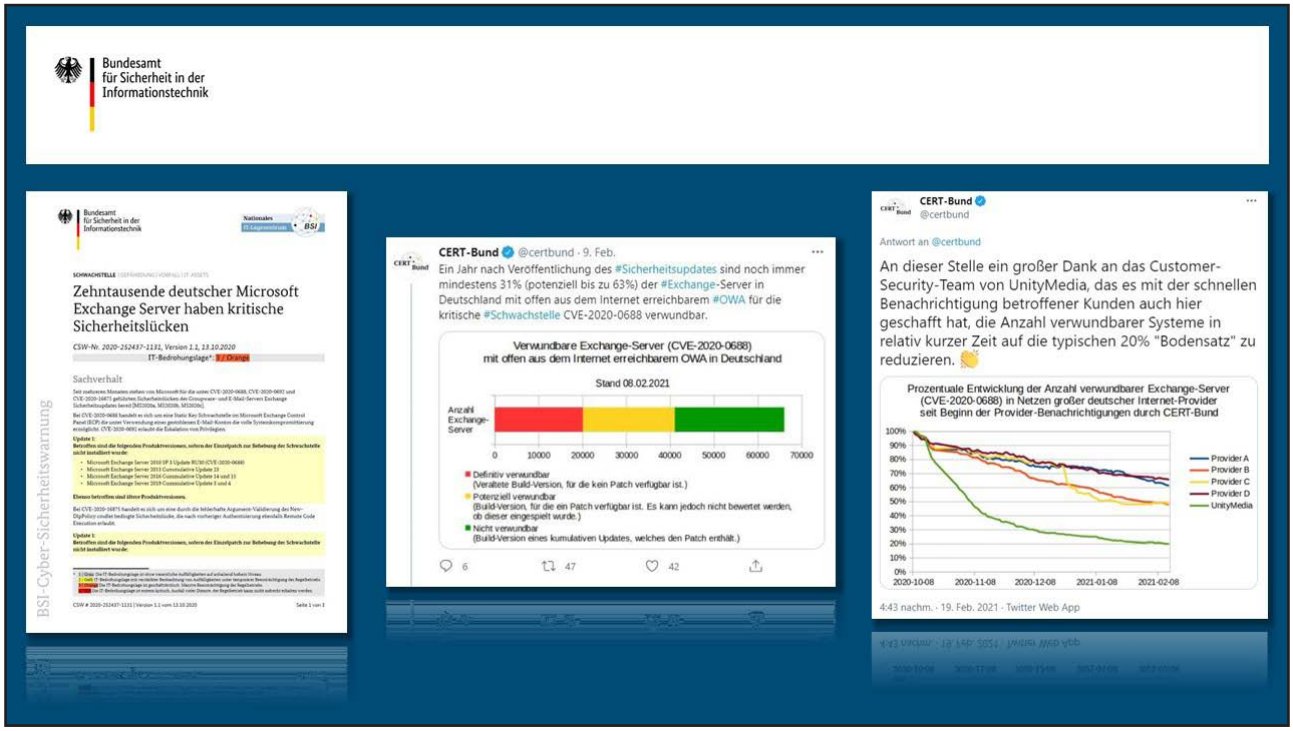
- Ausgenutzte Schwachstelle: CVE-2017-0144: Windows SMB Remote Code Execution Vulnerability („EternalBlue“)
- Durch Microsoft geschlossen am 14.03.2017
- Ausgenutzt durch WannaCry ab dem 12.05.2017

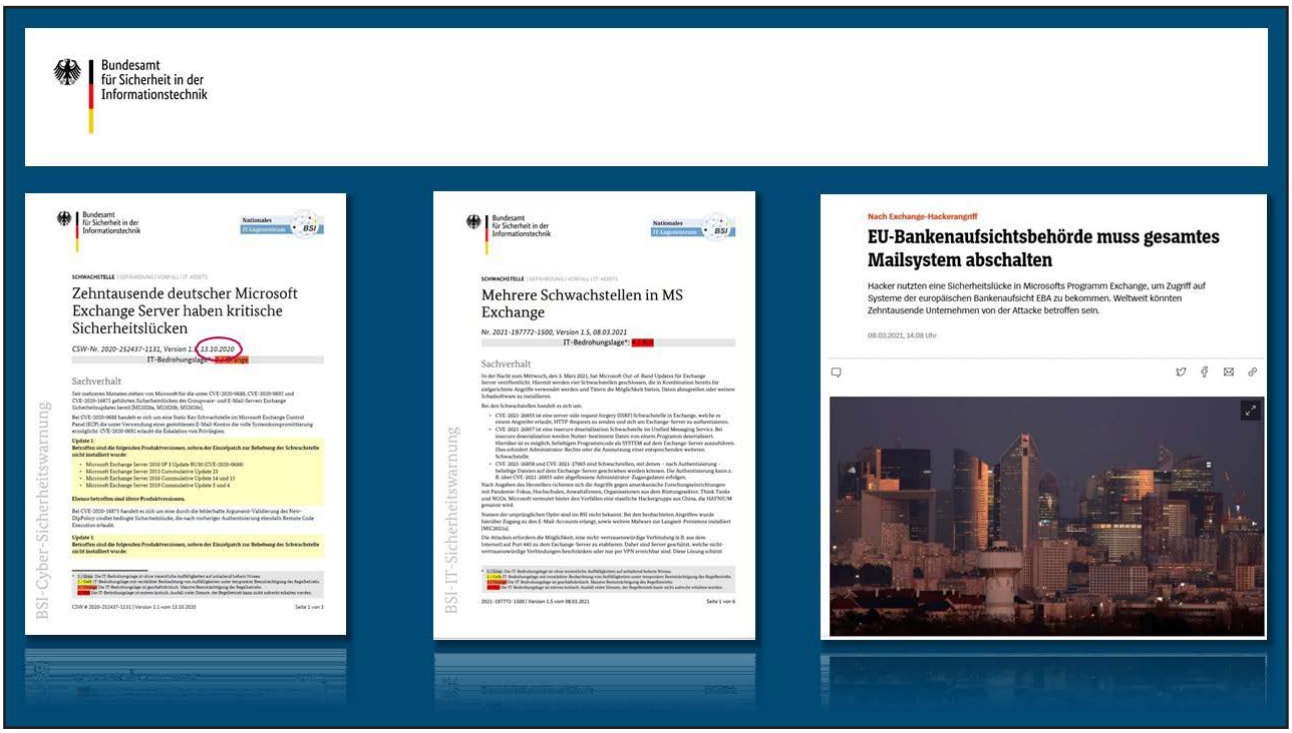
Kostenlose Gegenmaßnahme

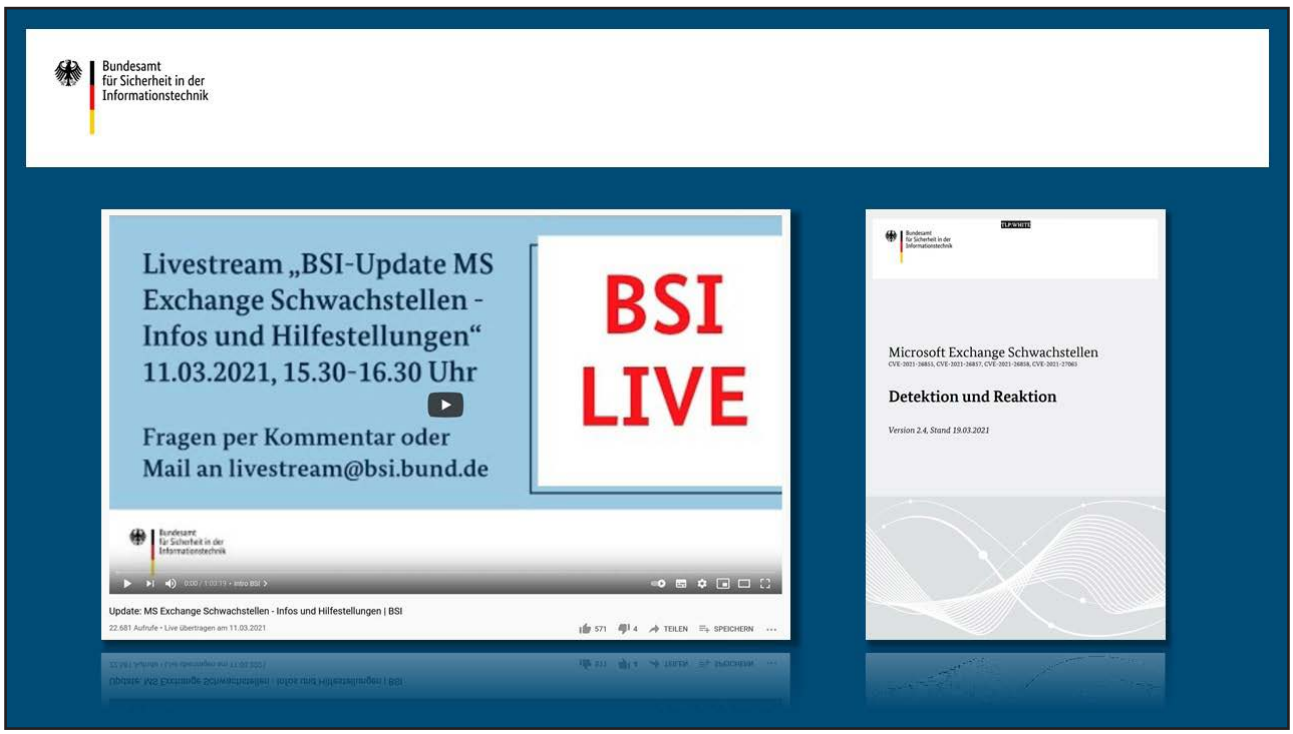
- Zeitnahes Einspielen von Updates
- Ggf. Umsetzen von Work-Arounds

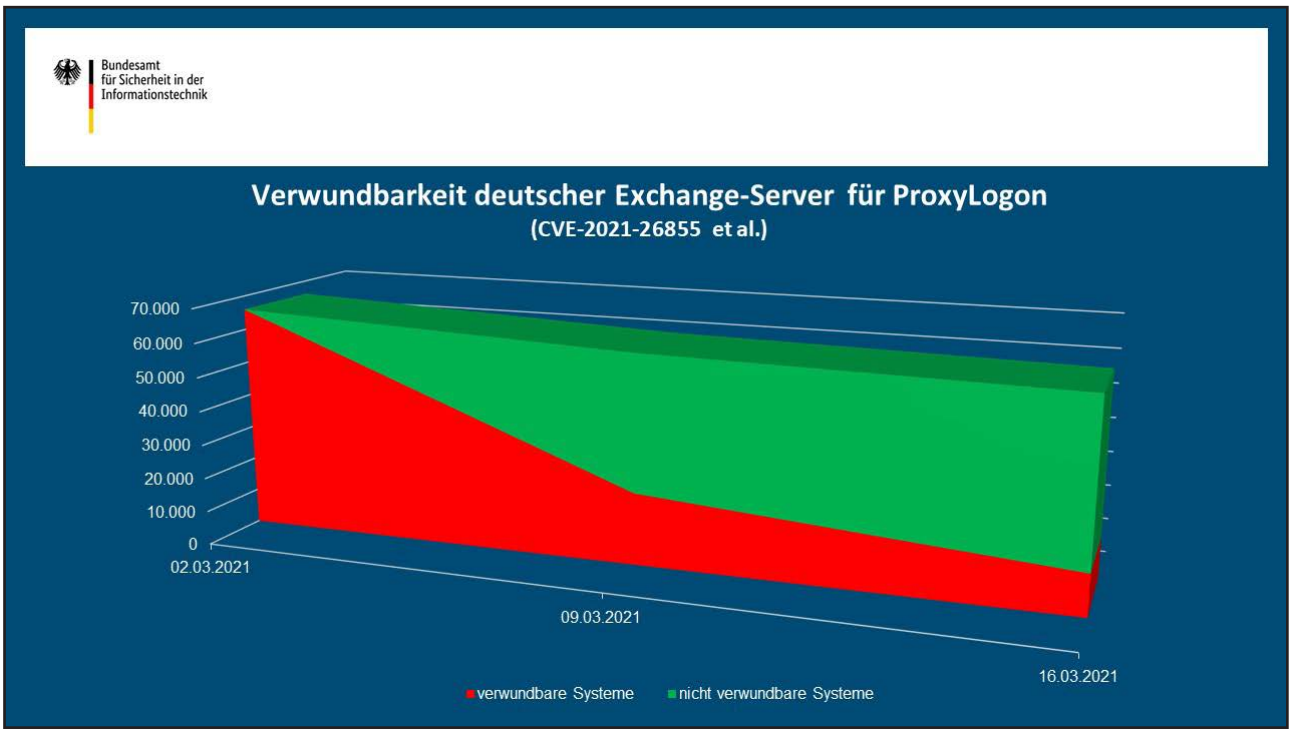
Bundesamt für Sicherheit in der Informationstechnik

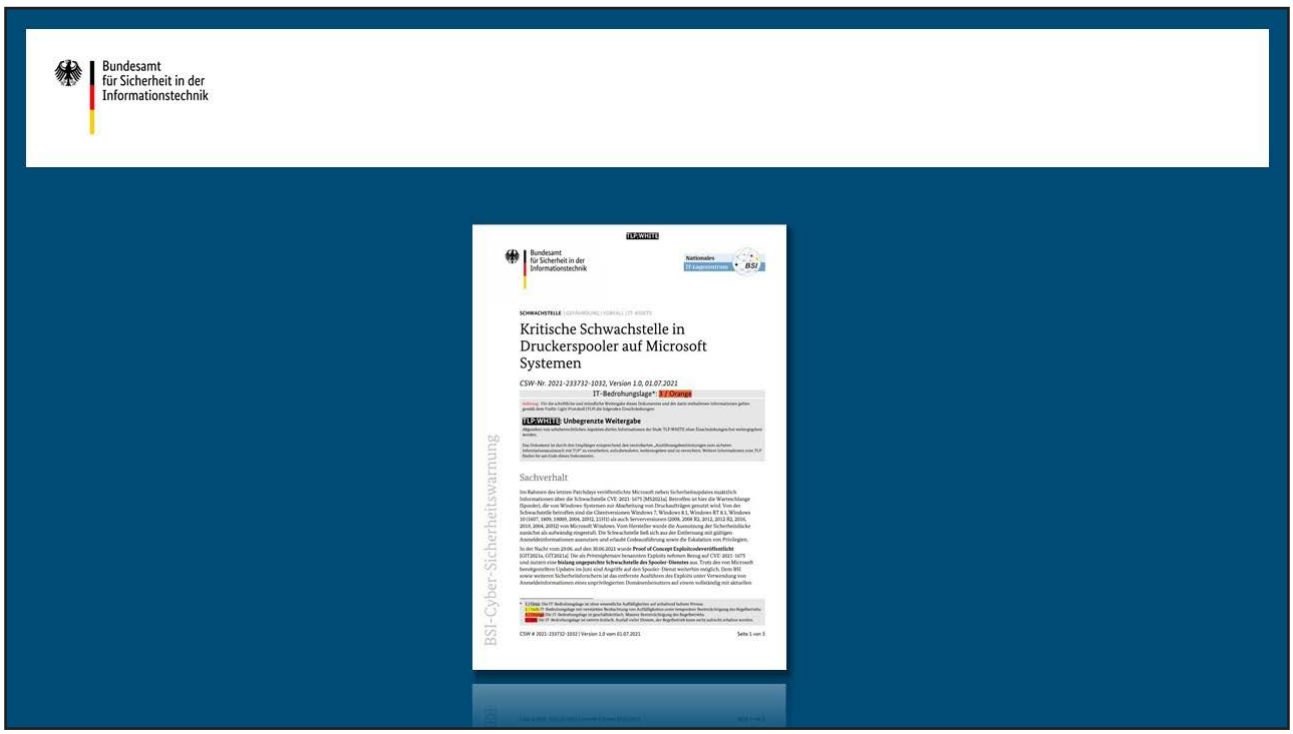

Bundesamt
für Sicherheit in der
Informationstechnik
CERT-Bund
@certbund
In der letzten Woche hat CERT-Bund 4.957 verwundbare #Citrix/#NetScaler VPN-Gateways an deutsche Netzbetreiber gemeldet. Davon sind aktuell noch 3.338 verwundbar.
Verwundbare Citrix/NetScaler VPN-Gateways (CVE-2019-19781) in DE
Gesamtzahl seit 07.01.2020 als verwundbar gemeldet
davon Stand 13.01.2020 noch verwundbar
7:56 nachm. · 13. Jan. 2020 · Twitter Web App
42 Retweets 4 Zitierte Tweets 55 „Gefällt mir"-Angaben
CERT-Bund
@certbund
Parallel zur #Pressemitteilung vom 17.09. bsi.bund.de/DE/Presse/Pres... hat das @BSI_Bund die Geschäftsführungen aller deutschen #Unternehmen, die noch immer für #CVE-2019-19781 verwundbare #Citrix/#NetScaler #VPN-Gateways betrieben haben, per Briefpost angeschrieben.
Für CVE-2019-19781 verwundbare Citrix/NetScaler-Systeme in Deutschland
9:27 vorm. · 2. Okt. 2020 · Twitter Web App
28 Retweets 20 Zitierte Tweets 57 „Gefällt mir"-Angaben

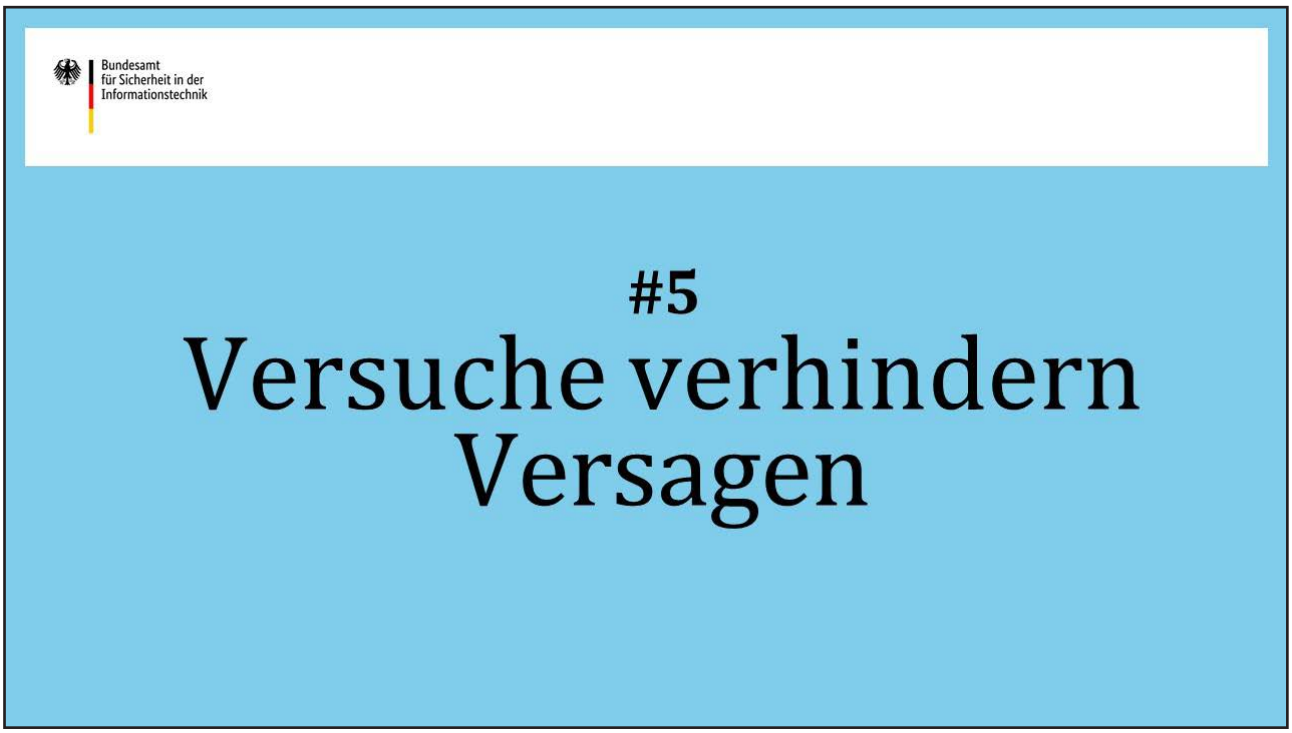

Bundesamt
für Sicherheit in der
Informationstechnik
BSI-Cyber-Sicherheitswarnung
Zehntausende deutscher Microsoft Exchange Server haben kritische Sicherheitslücken
Sachverhalt
CERT-Bund @certbund · 9. Feb.
Ein Jahr nach Veröffentlichung des #Sicherheitsupdates sind noch immer mindestens 31% (potenziell bis zu 63%) der #Exchange-Server in Deutschland mit offen aus dem Internet erreichbarem #OWA für die kritische #Schwachstelle CVE-2020-0688 verwundbar.
Verwundbare Exchange-Server (CVE-2020-0688) mit offen aus dem Internet erreichbarem OWA in Deutschland
Stand 08.02.2021
Anzahl Exchange-Server
Definitiv verwundbar (Veraltete Build-Version, für die kein Patch verfügbar ist.)
Potenziell verwundbar (Build-Version, für die ein Patch verfügbar ist. Es kann jedoch nicht bewertet werden, ob dieser eingespielt wurde.)
Nicht verwundbar (Build-Version eines kumulativen Updates, welches den Patch enthält.)
CERT-Bund
@certbund
Antwort an @certbund
An dieser Stelle ein großer Dank an das Customer-Security-Team von UnityMedia, das es mit der schnellen Benachrichtigung betroffener Kunden auch hier geschafft hat, die Anzahl verwundbarer Systeme in relativ kurzer Zeit auf die typischen 20% "Bodensatz" zu reduzieren.
Prozentuale Entwicklung der Anzahl verwundbarer Exchange-Server (CVE-2020-0688) in Netzen großer deutscher Internet-Provider seit Beginn der Provider-Benachrichtigungen durch CERT-Bund
Provider A
Provider B
Provider C
Provider D
UnityMedia
4:43 nachm. · 19. Feb. 2021 · Twitter Web App


Bundesamt
für Sicherheit in der
Informationstechnik
BSI-Cyber-Sicherheitswarnung
Zehntausende deutscher Microsoft Exchange Server haben kritische Sicherheitslücken
Sachverhalt
BSI-IT-Sicherheitswarnung
Mehrere Schwachstellen in MS Exchange
Sachverhalt
Nach Exchange-Hackerangriff
EU-Bankenaufsichtsbehörde muss gesamtes Mailsystem abschalten
Hacker nutzten eine Sicherheitslücke in Microsofts Programm Exchange, um Zugriff auf Systeme der europäischen Bankenaufsicht EBA zu bekommen. Weltweit könnten Zehntausende Unternehmen von der Attacke betroffen sein.


Bundesamt
für Sicherheit in der
Informationstechnik
Livestream „BSI-Update MS Exchange Schwachstellen - Infos und Hilfestellungen“
11.03.2021, 15.30-16.30 Uhr
Fragen per Kommentar oder Mail an livestream@bsi.bund.de
BSI LIVE
Update: MS Exchange Schwachstellen - Infos und Hilfestellungen | BSI
TLP-WHITE
Microsoft Exchange Schwachstellen
Detektion und Reaktion
Version 2.4, Stand 19.03.2021


Bundesamt
für Sicherheit in der
Informationstechnik
Verwundbarkeit deutscher Exchange-Server für ProxyLogon
(CVE-2021-26855 et al.)
70.000
60.000
50.000
40.000
30.000
20.000
10.000
0
02.03.2021
09.03.2021
16.03.2021
verwundbare Systeme
nicht verwundbare Systeme


Bundesamt
für Sicherheit in der
Informationstechnik
BSI-Cyber-Sicherheitswarnung
Kritische Schwachstelle in Druckerspooler auf Microsoft Systemen
CSW-Nr. 2021-233732-1032, Version 1.0, 01.07.2021
IT-Bedrohungslage*: 3 / Orange
TLP:WHITE: Unbegrenzte Weitergabe
Sachverhalt

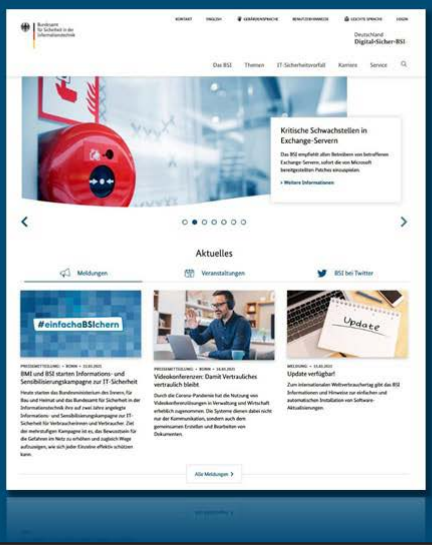

Bundesamt
für Sicherheit in der
Informationstechnik
#5
Versuche verhindern
Versagen


Bundesamt
für Sicherheit in der
Informationstechnik
Üben Sie den Ernstfall!

Bundesamt
für Sicherheit in der
Informationstechnik

Nutzen Sie das BSI!

Bundesamt
für Sicherheit in der
Informationstechnik



Gut vernetzt - Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit ist eine Initiative des Bundes der Informationstechnik (BSI).

Sie bietet eine Kooperationsbasis zwischen:

→Staat,
→Wirtschaft,
→Herstellern und
→Forschung

Angebote für Unternehmen und Institutionen

NETZWERKE SCHÜTZEN NETZWERKE
www.allianz-fuer-cybersicherheit.de

Allianz für Cyber-Sicherheit

Informationen erhalten	Erfahrungen austauschen	Kompetenzen erwerben
Online-Informationspool: • BSI-Warnungen • Aktuelle Lagebilder • Lösungshinweise und Anleitungen • Hintergrund-wissen • Veranstaltungs-dokumentation	Cyber-Sicherheits-Tage Umfrage ERFA-Kreise Experten-Kreise	Übungszentrum Netzverteidigung **Angebote der Partner:** • Schulungen und Workshops • Analysen und Erstberatung • Pen-Tests • Tools

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Manuel Bach
Leiter Referat „Cyber-Sicherheit für Kleine und Mittlere Unternehmen (KMU)“

manuel.bach@bsi.bund.de
Tel. +49 (0) 228 9582 5941
Fax +49 (0) 228 10 9582 5941

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Bundesamt für Sicherheit in der Informationstechnik

Seite 43


erste Adresse
lie Unternehmen
nserer Region.

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)

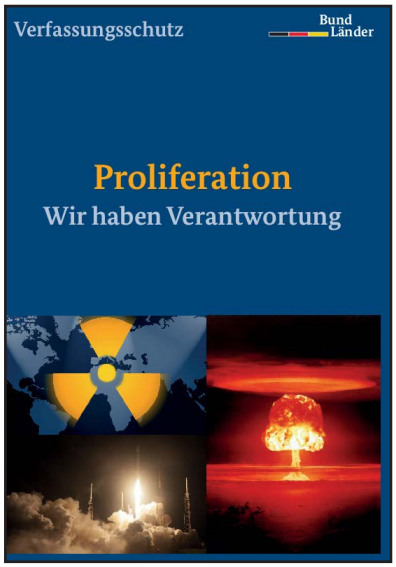
Tagungsdokumentation

3. Wirtschaftsschutztag Sachsen-Anhalt
„Neue Risiken, neue Bedrohungen“

Wirtschaftsschutztag am 26. November 2019
in Magdeburg

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

- Unsere Themen.
- Elektronische Angriffe - Gefahren für Informations- und Kommunikationstechnik.
- Cloud Computing. Was KMU wissen und beachten sollten.
- Fokus Wissenschaft. Gefahren für Forschung und Lehre.
- Industrie 4.0. Herausforderungen neuer Technologien.
- Geschäftsreisen. Sicherheit bei Auslandsreisen.
- Know-how-Schutz. Identifizieren. Bewerten. Schützen.
- Besuchermanagement. Umgang mit Besuchern und Fremdpersonal.
- Personalauswahl. Loyalität als Sicherheitsgewinn.
- Sicherheitslücke Mensch. Gefahr durch Innentäter.
- Social Media. Risiken durch soziale Netzwerke



Proliferation
„Wir haben Verantwortung“

Gemeinsame Broschüre des Bundesamtes für Verfassungsschutz und der Verfassungsschutzbehörden der Länder

Verfassungsschutzbericht

Jährlicher Bericht des Verfassungsschutzes 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.

Tagungsdokumentation

„Linksextremismus: Neue Entwicklungen

jenseits von Marx, Engels und Lenin“

Fachtagung am 23. September 2020

in Magdeburg

Broschüre

„Extremistisch und gesetzeskonform?

Eine Informationsbroschüre zum

„Legalistischen Islamismus““

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 Nachtweide 82 39124 Magdeburg Tel.: 0391 567 3900 E-Mail: verfassungsschutz@mi.sachsen-anhalt.de www.mi.sachsen-anhalt.de/verfassungsschutz
Druck:	Statistisches Landesamt Sachsen-Anhalt Merseburger Straße 2, 06110 Halle (Saale)
Fotos Umschlag:	fotomek– stock.adobe.com
Bildnachweis:	Laurence Chaperon (Seite 3) Ministerium für Inneres und Sport des Landes Sachsen-Anhalt (Seite 8, 22, 48-50) ihk.halle.de (Seite 9) Prof. Dr. M. Angela Sasse (Seite 11)

Stand: Oktober 2022

SACHSEN-ANHALT
Ministerium für Inneres und Sport

#moderndenken