PROVINZIAL

Sicherheit vor den Folgen von Cyberkriminalität

Ihr PROVINZIAL Schutzschild

Wolfgang Henkes
Direktionsbevollmächtigter Marktbearbeitung Kommunen / Sparkassen / Kirchen
Provinzial Nord Brandkasse Aktiengesellschaft

Cyber – Kriminalität ein reales Risiko für Verwaltungen und Unternehmen

Cyber - Kriminalität wird immer noch oft unterschätzt, dabei ist es inzwischen ein alltägliches Phänomen.

Jeder Betrieb verfügt über Daten die für Hacker von hohem Interesse sind.

Kontodaten und Kreditkartendaten
Gesundheitsdaten
Personaldaten

Die Hacker dringen in die Systeme ein…

nutzen Ihre Daten für kriminelle Zwecke
greifen in die Steuerung Ihrer Produktionen ein und legen den Betrieb lahm
stehlen Konstruktions- und Entwicklungsdaten

BSI-Lagebericht

Immer mehr Cyberangriffe in Deutschland

Stand: 09.11.2016 14:19 Uhr

Cyberattacken auf IT-Systeme haben drastisch zugenommen. Immer häufiger werden Behörden oder Unternehmen Ziel von Erpresser-Software, die Daten verschlüsselt und nur gegen Lösegeld wieder freigibt. Eine neue schnelle Eingreiftruppe soll nun wichtigen Einrichtungen im Notfall helfen.

Große Zunahme von Schadprogrammen

Sorgen machen den Experten die exorbitante Zunahme schädlicher Programme. Täglich würden rund 380.000 neue Varianten von Schadprogrammen entdeckt. Die Anzahl von Spam-Nachrichten mit Schadsoftware im Anhang sei im ersten Halbjahr 2016 explosionsartig um 1270 Prozent im Vergleich zum Vorjahr gestiegen. Gleichzeitig verlören bisherige klassische Abwehrmaßnahmen an Wirksamkeit. Die Spam-Aktivitäten hätten um etwa 73 Prozent zugelegt.

Die Risiken der Vernetzung – Cyber Kriminalität boomt ! PROVINZIAL

Cyberkriminalität in Deutschland

2015 mehr als 40 Millionen Euro Schaden

Mindestens 45.000 Fälle von Computer- und Internetkriminalität hat es 2015 in Deutschland gegeben, meldet das Bundeskriminalamt. Sein Chef Holger Münch hat sich auch zur Bedeutung des sogenannten Darknets geäußert.

SPIEGEL ONLINE
NETZWELT
Mittwoch, **27.07.2016**

GDV 2014

250 Mio. **Schadprogramme** gibt es heute weltweit und 300.000 Varianten kommen **jeden Tag** neu dazu

Es gibt schätzungsweise 60 global agierende **Cybercrime-Organisationen**

Deutschland hat 2013 den traurigen **1. Platz bei den Schäden** belegt, die durch Cyberangriffe verursacht werden – insgesamt

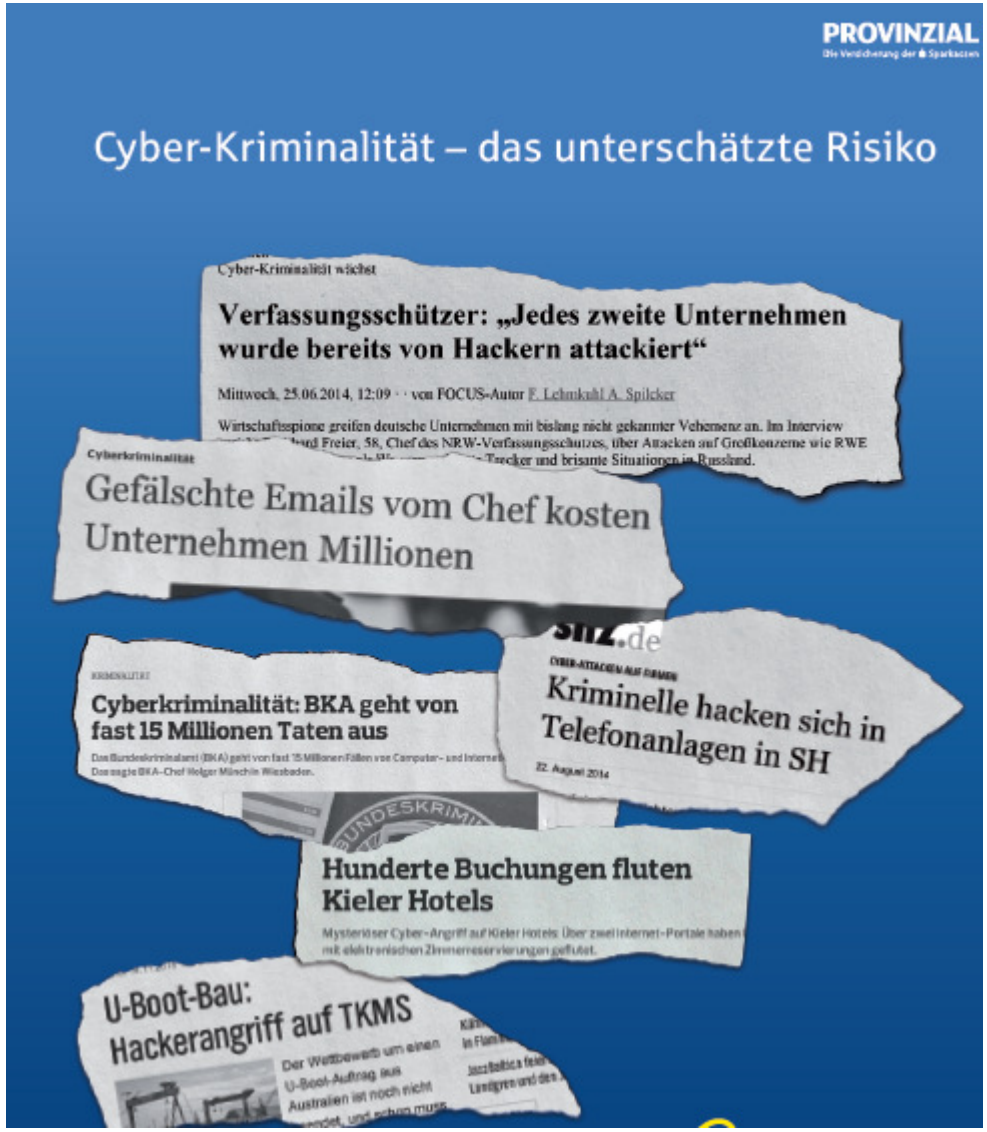
46 Mrd. €

2016 sind es 560 Mio. Schadprogramme

380.000 neue jeden Tag und ca. 50 Mrd. Euro Schaden

Das Brandrisiko des 21 Jahrhunderts

PROVINZIAL



APT/Advanced Persistent Threat

Backdoor

Bot-Net

Clickjacking

Cross-Site-Scripting

Denial-of-Service Attacke/Dos

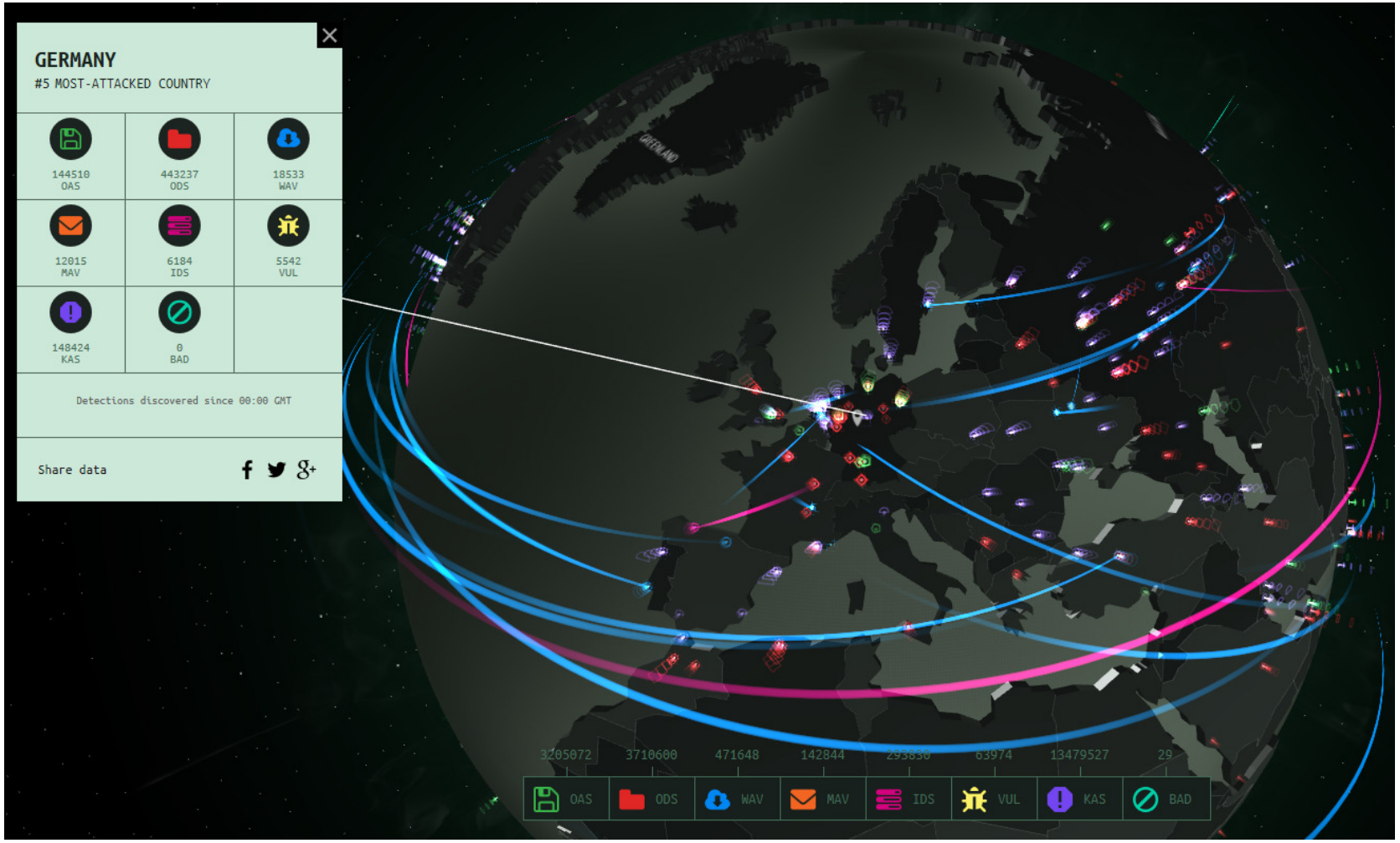
Injection -Attacken

MAC –Spoofing

Man-in-the-middle Attacke

Keylogger

usw.



https://cybermap.kaspersky.com/

„Datenklau ist lukrativer als der weltweite Drogenhandel“

Russische Hacker haben 1,2 Milliarden Internet-Passwörter gestohlen. Nur die Spitze des Eisberges, sagt Datensicherheitsexperte Thorsten Urbanski. Krimineller Datenhandel sei längst ein Riesengeschäft.

Montag, 11. April 2016

Wirtschafts Woche

Datenschutz -verletzung

Hacker greifen Zulassungsbehörden in Hessen an

Frankfurter Allgemeine
Rhein-Main

Unbekannte greifen das Computersystem von Kfz-Zulassungsstellen in Hessen und Rheinland-Pfalz an. Das Unternehmen, das für die IT in den Behörden zuständig ist, spricht von einem Hackerangriff. Was wollten die Cyber-Kriminellen eigentlich?

22.06.2015

Hacker-Angriff

Ransomware-Virus legt Krankenhaus lahm

heise online 12.02.2016 12:48 Uhr – Detlef Borchers

Cyber-Erpressung

(Bild: heise Security)


SPIEGEL ONLINE NETZWELT
Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | estages | Karriere | Uni | Reise | Auto | Stil
Nachrichten > Netzwelt > Web > Computerviren > Ransomware Teslacrypt:
Viren + Trojaner
Tesla-Crypt: Erpressung mit Troj ng zahlte Lösegeld
Von Jörg Diehl und Björn Hengst
Ein Erpressungs-Trojaner hatte die Stadtverwaltung im unterfränkischen Dettelbach weitgehend lahmgelegt. Die Behörde sah sich gezwungen, das verlangte Lösegeld zu zahlen.
Teilen
Twittern
E-Mail
Donnerstag, 03.03.2016 – 17:42 Uhr

IT-Sicherheit

17.10.2015 14:23 Uhr

Immer mehr Hackerangriffe auf Banken

Hackerangriffe auf Unternehmen häufen sich seit Jahren. Nun spricht die Finanzaufsicht BaFin von zunehmenden Angriffen auf Banken. Belastbare Zahlen hat man aber nicht.

Die Frankfurter Skyline unter Belagerung: Zahlreiche Hackerangriffe richten sich gegen Banken und Sparkassen. FOTO: CHRISTOPH SCHMIDT/DPA

golem.de
IT-NEWS FÜR PROFIS

DDos-Attacken

LIEFERHELD GEGEN LIEFERANDO

DoS-Attacken im Konkurrenzkampf zwischen Pizzaplattformen

Das Landeskriminalamt hat die Büroräume von Lieferheld.de wegen einer Anzeige von Lieferando durchsuchen lassen. Lieferheld weist die Vorwürfe zurück. Zwischen den Metasuchmaschinen für Essenslieferungen läuft eine erbitterte Auseinandersetzung.

Lieferheld.de soll seinen Konkurrenten Lieferando mit DoS-Attacken lahmgelegt haben. Das berichtet das Nachrichtenmagazin Der Spiegel in seiner Printausgabe. Danach sollen im vorigen Jahr wiederholt die Server von Lieferando stundenlang gezielt überlastet worden sein. Der Angreifer hätte sich zudem an einem Sonntag im Dezember 2011 in den Mitgliederbereich eingeloggt und dort rechenintensive Vorgänge ausgelöst. Die Server gingen offline.

(Bild: Rodger Bosch/AFP/Getty Images)

Datum:	23.4.2012, 12:47
Autor:	Achim Sawall
Themen:	DoS, Bundesregierung, Lieferdienst, Suchmaschine, Server, Internet
Teilen:	0 · 152 · 50 · 39

Leitartikel

Wir stehen erst am Anfang

Angriffe aus dem Internet nehmen zu

Die Wochen um Weihnachten sind eine schöne Zeit für Familien, für die Wirtschaft – und für Cyberkriminelle. Traditionell geht die Zahl der versendeten Spam-E-Mails zum Ende eines Jahres nach oben. Oft mit im Paket: mit Viren verseuchte Anhänge oder Links zu manipulierten Internetseiten. Die Absender wollen Nutzer im Festtagsstress um Daten oder Geld erleichtern. Oder um beides.

Doch Schadsoftware kommt nicht nur per Mail – pausenlos wabern schädliche Programme durch das Internet und suchen nach Einfallstoren, um Systeme zu übernehmen. Von Regierungen, Behörden, Unternehmen oder Privatnutzern. 1000 Angriffe pro Monat auf die Systeme des Landes klingt viel. Doch wir stehen erst am Anfang. Täglich werden 380 000 neue Schadprogrammvarianten gesichtet, das zeigt der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik.

Angst machen sollte uns das nicht. Uns zum Handeln motivieren hingegen schon. Kein Unternehmen kann auf Informationstechnik verzichten. Keine Behörde komplett offline bleiben. Und wenn man Branchenexperten glaubt, können Otto-Normal-Bürger sich auf lange Sicht nicht gegen vernetzte Technik im Haus oder im Auto wehren.

Doch all die neuen Zugänge zu Systemen müssen wir schützen. Und zwar besser als bisher. Indem wir als Nutzer nicht achtlos im Netz surfen und die Schutzprogramme auf dem Rechner aktuell halten. Und indem Behörden und Unternehmen auf Experten setzen. Das kostet Geld. Aber geklaute Daten und verlorenes Vertrauen kann sich erst recht niemand leisten.

Das Internet geht nicht mehr weg. Und das ist auch gut so. Wir alle müssen aber schleunigst lernen, dass wir uns nicht auf bisher Gelerntem ausruhen können. Das machen auch die Kriminellen nicht. Die Angriffe werden besser und häufiger. Wöchentlich, täglich, stündlich…– egal ob Weihnachten ist oder nicht.

Anja Christiansen ist Mitglied unserer Online-Redaktion
ANJ@SHZ.DE

SCHLESWIG-HOLSTEINISCHE
LANDESZEITUNG
UNABHÄNGIGE TAGESZEITUNG IN SCHLESWIG-HOLSTEIN gegründet 1867 NACHRICHTEN FÜR RENDSBURG UND RENDSBURG-ECKERNFÖRDE

W.SHZ.DE MONTAG, 9. JANUAR 2017 – NR. 7 – € 1,60

Erpresser-Angriffe von Hackern immer massiver

Auch Landesbehörden betroffen / Attacken wurden abgewehrt / IT-Sicherheit oberstes Gebot

KIEL Während der Streit zwischen den USA und Russland über Cyber-Attacken im amerikanischen Wahlkampf an Schärfe zunimmt, wächst die Angst vor Hacker-Angriffen auch im Norden. Allein der IT-Dienstleister Dataport, der in Schleswig-Holstein und Hamburg 70 000 Rechner aller Landesbehörden und teils von Kommunalverwaltungen betreut, musste im alten Jahr per Virenscanner rund 1000 Hacker-Angriffe abwehren.

„Vor allem die Angriffe mit Erpressungs-Trojanern sind 2016 massiv geworden", beobachtet Dataport-Sprecherin Britta Heinrich. Dabei tarnen sich Schadprogramme als Anhang einer E-Mail, etwa als Bewerbungsschreiben. Geöffnet, machen sie nicht nur den Rechner unbrauchbar – sondern greifen auf die gespeicherten Daten zu. Diese nehmen die Hacker-Programme als „Geisel" – und bieten dem Rechner-Benutzer an, bei Überweisung eines Geldbetrags die Beschädigung rückgängig zu machen. Auch drei PCs des Landespolizeiamts und einer des Statistikamts Nord waren davon im Dezember laut Dataport betroffen. Den Fachleuten zufolge handelte es sich bisher stets um Zufallstreffer von wahllosen Massenangriffen. Gezielte Angriffe sind nicht bekannt.

„Wenn man sich vornimmt, einer Verwaltung Schaden zuzufügen, sind viele nicht so aufgestellt, dass sie sich wehren können", warnt die Landes-Datenschutzbeauftragte Marit Hansen. „Das Sicherheitsrisiko ist gestiegen. Bei den Schutzvorkehrungen leben viele von der Hand in den Mund". Denn die Angreifer hecken immer neue Tricks aus. Allein bei den zehn meistverwendeten Software-Programmen ist die Zahl der bekannten Schwachstellen binnen zweier Jahre von 1000 auf 1600 gestiegen. „IT-Sicherheit darf nicht nur nebenbei und zufällig laufen. Sie braucht Ressourcen, und das kostet Geld", ruft Hansen zu Investitionen auf. Sie warnt davor, dass die Steuerung des Energieverbrauchs in Privathaushalten über das Smartphone zum neuen Einfallstor für Daten-Angriffe wird.

> *„Bei den Schutzvorkehrungen leben viele von der Hand in den Mund."*
> **Marit Hansen**
> Landes-Datenschutzbeauftragte

„Wir haben schon von Firmen gehört, die auf Grund von Angriffen praktisch handlungsunfähig waren", heißt es bei der IHK Flensburg. Sebastian Schulze, Sprecher des Unternehmensverbands Nord, verdeutlicht: „Gerade kleine Unternehmen, die das Thema ganz [illegible] Bank durch [illegible] hungsszenarien bedarf."

Beim [illegible] Krisenmanagement [illegible] griffe so [illegible] Krisen-Szenarien [illegible] werks-Ex[illegible] terhält [illegible] lange [illegible] Kommunikation.

Das Landeskriminalamt [illegible] über keine aussagekräftigen [illegible] zu strafrechtlich relevanten [illegible] cker-Angriffen – verweist [illegible] auf Ermittlungserfolge. Dazu zählten mehrere Durchsuchungen bei Tätern, die gestohlene Daten – etwa für Kreditkarten – im Internet in Untergrund-Foren verkaufen oder für Online-Drogenhandel nutzen wollten. In einem extrem aufwändigen Verfahren hat das LKA unlängst einen Hacker identifiziert, der in die Datenbanken von Unternehmen aus ganz Deutschland eindrang und die Firmen dann mit der Drohung erpresste, diese Daten zu veröffentlichen. *Frank Jung*

Leitartikel Seite 2

Cyber-Erpressung

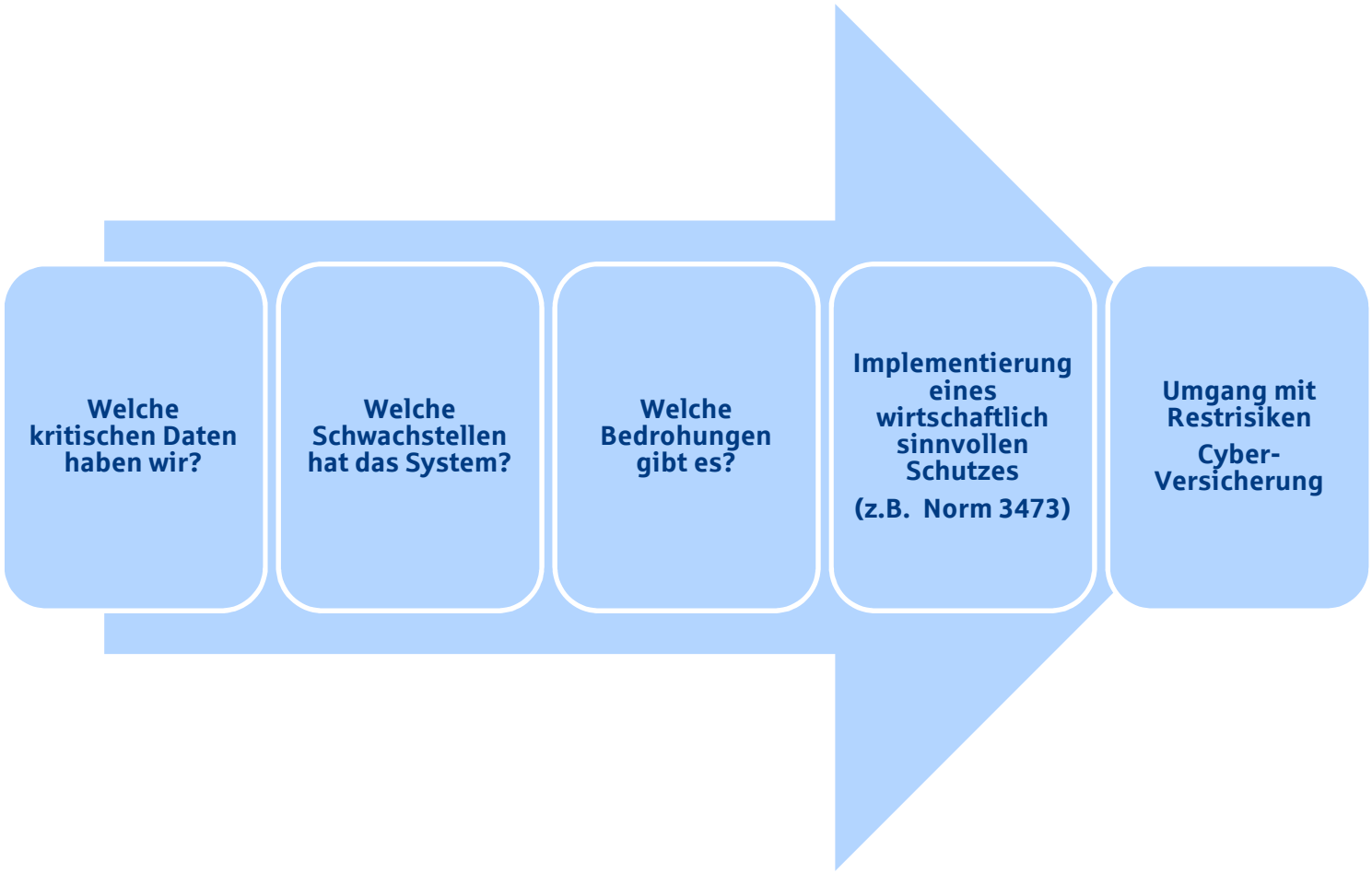
Phasen eines Cyber-Angriffes

Ausspähen	Beschaffung und Analyse öffentlicher und interner Informationen z.B. über Organisationsstruktur, strategische Positionen, Zugriffsrechte, Zielpersonen
Taktik	Festlegung der Angriffstaktik, z.B. Welche Malware ist geeignet? Welche Maßnahmen zur Verschleierung?
Lieferung	Infizierung des ausgewählten Systems / Übertragung des Angriffswerkzeuges in die Zielumgebung. Z.B. auch durch Social Engeneering
Schwach-stelle	Mit Hilfe des Angriffswerkzeuges wird in der Zielumgebung nach Schwachstellen gescannt. Passenden Instrumente werden nachgeladen.
Installation	Installation eines Command and Control Tools
C & C	Übernahme der C & C über Remote-Verbindung
Ausführung	Ausführung der geplanten Aktionen. Z.B. Datendiebstahl, -manipulation, Verursachung von Systemausfällen, Verteilung von Malware an Dritte, Nutzung Ressourcen

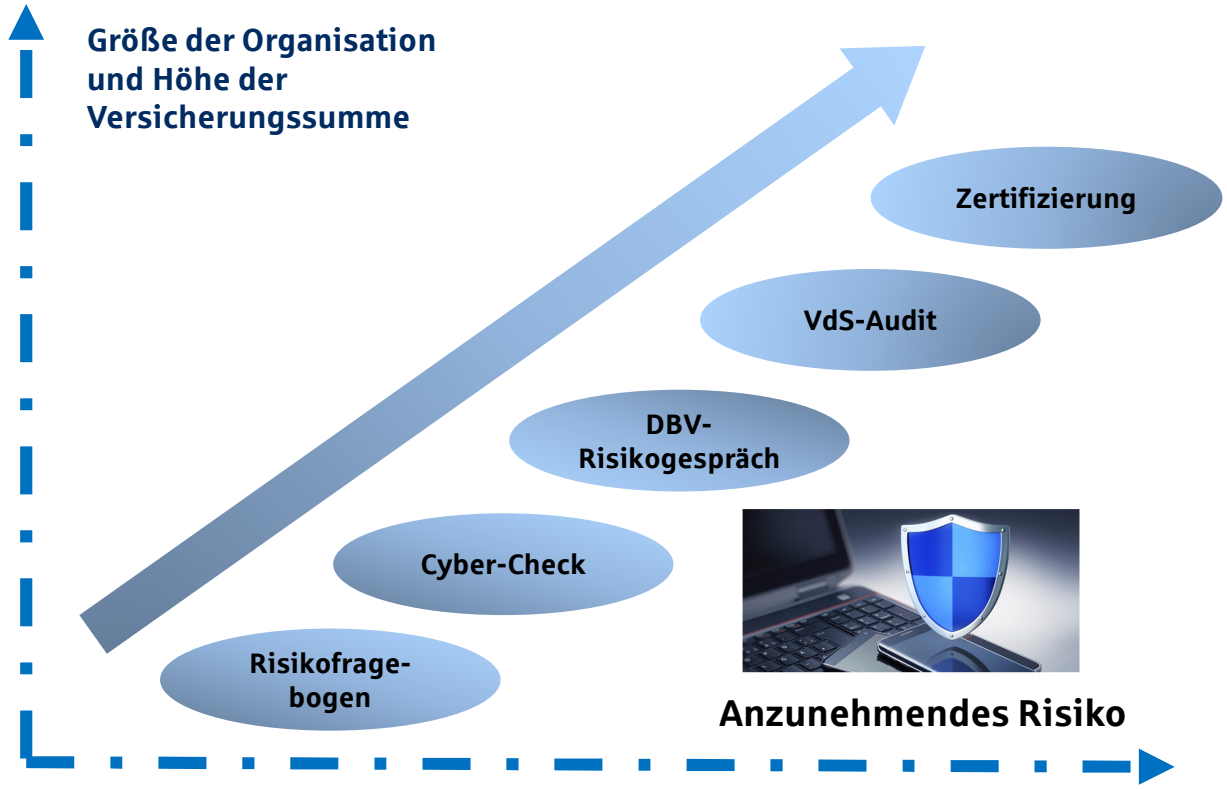
Wer sind die Angreifer?

Bedrohungs-matrix	Cyber-Crime	Script-Kiddies	Cyber-Spionage	Hackti-vismus	Interne Täter
Motivation	Geld	Spaß, Neugier	strategisch	Ethik, Politik	Rache, Geldnot
Zielauswahl	individuell, Zufällig	zufällig, politisch	Individuell	ideologisch, politisch	Arbeit-geber
Organisation	sehr hoch	teilweise	sehr hoch bis perfekt	strukturiert	kaum
Kompetenz	hoch	gering bis hoch	sehr hoch	mittel bis hoch	hoch, Insider-wissen

Von schützenswerten Daten zur Cyber-Versicherung



Risikolage, Versicherungssumme und Unternehmensgröße werden berücksichtigt



Die Cyber-Versicherung der Provinzial

Cyber –Check auf der Provinzial Homepage

PROVINZIAL

PROVINZIAL
Die Versicherung der Sparkassen

Versicherungen Branchen Service

Suchen ...

Unsere Cyber-Versicherung - Ihr Schutzschild

Wir bieten im Rahmen von modular wählbaren Bausteinen Versicherungsschutz bei Schäden, die durch eine Verletzung der Informationssicherheit auftreten. Den Versicherungsschutz stellen wir gemeinsam mit Ihnen nach den Bedürfnissen Ihres Unternehmens zusammen.
Als starker Partner sichern wir Sie nicht nur finanziell ab. Wir sorgen auch für ein verlässliches Krisenmanagement, wehren unberechtigte Ansprüche gegen Sie ab und unterstützen Sie, sollte es zu einem Prozess kommen.

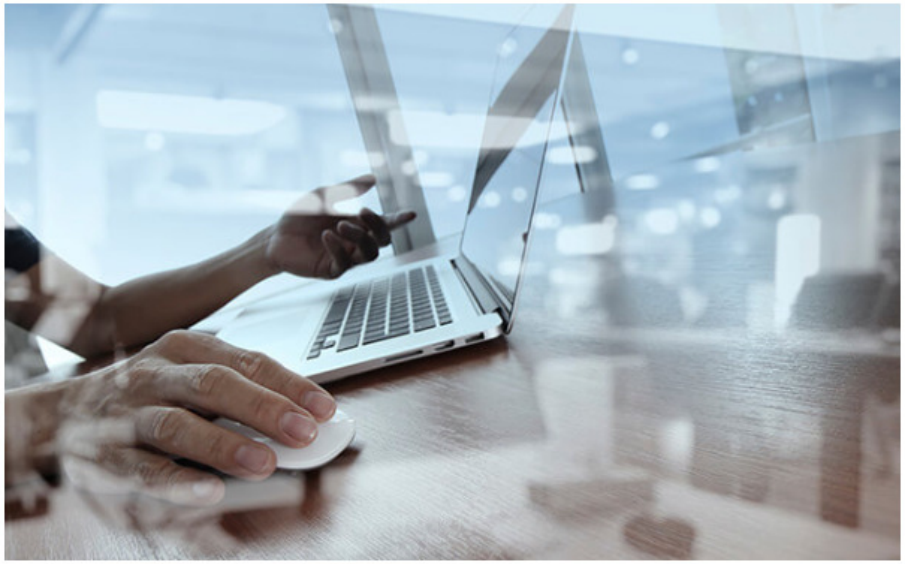
> Führen Sie hier Ihren Cyber-Check durch

Jetzt beraten lassen

Die Provinzial: Der richtige Partner für Ihr Unternehmen

Cyber-Versicherung → Bausteine

PROVINZIAL



Eigenschäden

- Kosten für die Wiederherstellung der Daten, der Systeme und des Netzwerkes nach einem Hackerangriff
- Kosten für IT-Forensiker, die den Sachverhalte schnell aufklären und gerichtsverwertbar dokumentieren
- Kosten für Krisenmanagement und PR-Maßnahmen nach einem Hackerangriff
- Kosten für die Verbesserung der Sicherheit nach einem Hackerangriff in Abstimmung mit uns

Haftpflichtschäden

- Verstoß gegen gesetzliche oder vertragliche Bestimmungen zum Datenschutz,
- Verstoß gegen Geheimhaltungspflichten,
- Weiterverbreitung von Computerviren an Dritte,
- Verletzung von Persönlichkeitsrechten nach einem Hacker-Angriff,
- Verstoß gegen E-Payment-Vereinbarungen (z. B. PC IDBS).

Cyber-Versicherung → Bausteine

PROVINZIAL

Vertrauensschäden

- z.B. Eingriffe in Ihre Buchhaltung, die zu Kontoabbuchungen führen
- Entgangener Gewinn nach Verrat oder Ausspähung von Betriebs- und Geschäftsgeheimnissen
- Mitarbeiter werden getäuscht und bezahlen z.B. eine manipulierte Rechnung die per Email zugeschickt wurde.

Ertragsausfall

- kommt es z.B. aufgrund eines Virenangriffs zu einem Stillstand Ihrer Produktionsmaschinen, übernehmen wir die durch den Produktionsausfall entstehenden Kosten.
- die Haftzeit beträgt sechs Monate
- nur acht Stunden zeitlicher Selbstbehalt

Was Sie erwarten können

PROVINZIAL

Highlight: Soforthilfe im Krisenfall durch unseren Partner SEC-Consult (eines der international führenden Unternehmen im Bereich Informations- und Applikationssicherheitsicherheit)

SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

https://www.sec-consult.com

- Einsatz IT-forensischer Methoden zur Ursachenforschung
- sofortige rechtliche Beratung
- Wiederherstellung der (kritischen) IT-Systeme und der Daten
- Dokumentation des Ablaufs der Attacke und Schließung der Sicherheitslücke
- Abwehrkosten bei behördlichen Verfahren
- Weltweiten Versicherungsschutz (außer USA und Kanada)
- **Hotline der DASG (24/7/365)** → Deutsche Assistance Service Gesellschaft

VdS – Unser Partner in der Risikoanalyse

PROVINZIAL

VdS-Auszeichnung

Branchen-Oscar für VdS-Cyber-Security

VdS Vertrauen durch Sicherheit

Der Innovation Award der Weltleitmesse für Sicherheit, der Security in Essen, gilt als „Branchenoscar“ für besondere Leistungen in der Schadenverhütung. // Den goldenen Award in der Kategorie „Dienstleistungen“ erhielten die umfassenden Angebote von VdS zur Cyber-Security speziell für den Mittelstand.

Köln, 28. September 2016. Der Security Innovation Award, vergeben durch die Sicherheits-Weltleitmesse Security in Essen, ist als „Branchenoscar“ bekannt. Alle zwei Jahre werden so herausragende Leistungen für optimale Schadenverhütung gewürdigt. Die goldene und damit höchste Auszeichnung in der Kategorie „Dienstleistungen“ ging am gestrigen Abend an das junge Cyber-Security-Angebot von VdS: Die Richtlinien VdS 3473, den ersten IT-Sicherheitsstandard speziell für den Mittelstand, samt zugehöriger Leistungen wie dem kostenlosen Quick-Check, dem schnellen Quick-Audit inklusive Testat oder der VdS-Zertifizierung der Informationssicherheit von Unternehmen.

https://www.vds.de/cyber/

Der VdS-Standard 3473 stellt die Basis unserer Risikoanalyse dar

- geeignet für kleine und mittlere Unternehmen, den gehobenen Mittelstand und Verwaltungen
- einfache und schnelle Implementierung
- Freiheit für individuelle Regelungen
- die gesamte Informationsverarbeitung wird betrachtet
- kritische IT-Ressourcen werden ermittelt und geschützt
- Zertifizierung ist im Regelfall nicht erforderlich
- Begründete Abweichungen sind möglich

Ach, hätten wir doch…

Quelle: McAfee