# Assecuranzmakler GmbH

# Cyber-Risiken

## Inhaltsverzeichnis

*Dienstag, 1. März 2022*

***Wegen Ukraine-Unterstützung***

# Welche russische Cyber-Rache droht Deutschland?

## Aus Rache für empfindliche Sanktionen und Waffenlieferungen an die Ukraine fürchten Sicherheitsbehörden russische Hackerangriffe auf Deutschland. Gegen wen oder was könnten sich solche Attacken wenden? Wie wahrscheinlich sind sie und wie gefährlich könnte so eine Eskalation werden?

Russlands Präsident Putin hat dem Westen unverhohlen mit extremen Konsequenzen gedroht, sollte man es wagen, sich ihm in der Ukraine in den Weg zu stellen. Die Folgen würden so sein, wie man sie in der Geschichte noch nie gesehen hat, sagte er. Was genau er damit meint, weiß man wie so oft bei ihm nicht genau. Die weitreichenden Sanktionen und beschlossenen Waffenlieferungen an die Ukraine könnte er aber durchaus entsprechend auslegen. Einen Atomkrieg wird er deshalb zwar kaum auslösen, aber Sicherheitsexperten sehen eine relativ große Gefahr, dass sich Putin mit Cyberattacken rächen könnte.

### Sicherheitsbehörden bereiten sich vor

Dass der russische Präsident nicht vor Hackerangriffen auf Behörden, Infrastruktur und Unternehmen anderer Länder zurückschreckt, hat er immer wieder bewiesen. Auch Deutschland ließ er in der Vergangenheit schon mehrmals attackieren. Für westliche Ermittler gilt es unter anderem als erwiesen, dass Moskau auch 2015 Drahtzieher der Cyberattacken auf den Bundestag war, um sich für Sanktionen nach der russischen Annexion der Krim zu rächen. Zuletzt gingen der Invasion der Ukraine offenbar von Putin angeordnete Hackerangriffe voran.

Experten schätzen die Gefahr russischer Cyberattacken auf deutsche Ziele groß ein. Bundesinnenministerin Nancy Faeser sagte vergangene Woche, „die Sicherheitsbehörden hätten Schutzmaßnahmen zur Abwehr etwaiger Cyberattacken hochgefahren".

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seinen Eigenschutz und seine Krisenreaktion gestärkt sowie das Nationale IT-Krisenreaktionszentrum aktiviert. Außerdem habe man seine Zielgruppen, darunter die Bundesverwaltung, Betreiber Kritischer Infrastrukturen und weitere Organisationen und Unternehmen sensibilisiert und zu einer erhöhten Wachsamkeit und Reaktionsbereitschaft aufgerufen, teilte die Behörde mit. Man sehe zwar aktuell keine akute Gefährdung, erkenne aber eine erhöhte Bedrohungslage.

Die Zusammenarbeit des BSI mit Verfassungsschutz, Bundeskriminalamt und anderen Behörden und Einrichtungen wird vom Nationalen Cyber-Abwehrzentrum (Cyber-AZ) koordiniert.

### Es gibt viele mögliche Ziele

Grundsätzlich unterscheidet man dabei zwischen zwei Schutzbereichen. Bei den kritischen Infrastrukturen (KRITIS) handelt es sich um Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen. Deren Ausfall oder Beeinträchtigung hätte nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen.

Zur kritischen Infrastruktur gehören Wasser- und Energieversorgung, Ernährung, Finanz- und Versicherungswesen, der Gesundheitssektor, Informationstechnik und Telekommunikation, Transport und Verkehr, Staat und Verwaltung, Medien und Kultur und seit dem vergangenen Jahr auch die Siedlungsabfallentsorgung.

Der zweite Bereich sind Unternehmen im besonderen öffentlichen Interesse (UBI). Zu ihnen gehören Rüstungsbetriebe oder Firmen, die Produkte oder Komponenten herstellen, die bei der IT-Sicherheit staatlicher Verschlusssachen zum Einsatz kommen.

UBI sind laut BSI-Gesetz außerdem Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen des Landes gehören und daher von erheblicher volkswirtschaftlicher Bedeutung sind. Unter Umständen zählen auch deren Zulieferer dazu. Schließlich legt man noch besonderes Augenmerk auf Betriebe, wo bestimmte Mengen an gefährlichen Stoffen vorhanden sind.

## Umstrittene Rolle der Bundeswehr

Auch die Bundeswehr ist mit dem Kommando Cyber- und Informationsraum (CIR) im Cyber- AZ vertreten. Ihre Rolle ist allerdings umstritten. Unter anderem gilt auch in diesem Bereich, dass die Bundeswehr nur im Krisen- und Verteidigungsfall eingesetzt werden darf, der vom Bundesparlament festgestellt werden muss.

Wann das genau der Fall ist, ist nicht eindeutig geklärt. In einem Arbeitspapier der Bundesakademie für Sicherheitspolitik heißt es, „erst wenn ein Cyberangriff in seiner Intensität und seinen Auswirkungen einem bewaffneten Angriff gleicht, kann man völkerrechtlich von einem Angriff sprechen."

Eine völkerrechtliche Definition eines „bewaffneten Angriffs" gibt es zwar nicht. Das Arbeitspapier geht jedoch davon aus, dass dies der Fall ist, wenn Cyber-Operationen zu Toten sowie großflächiger materieller Zerstörung führen.

## Ohne Mandat nur Selbstverteidigung

Solange sie nicht selbst betroffen ist, ist die Abwehr von Hackerangriffen in Friedenszeiten grundsätzlich nicht Sache der Bundeswehr. Auch sogenannte Hackbacks zur Vergeltung eines Cyberangriffs sind vom Grundgesetz nur im Verteidigungsfall gedeckt, die neue Bundesregierung hat sie im Koalitionsvertrag ausgeschlossen. Nicht ganz klar ist auch, wie weit die Befugnisse des CIR zur militärischen Aufklärung gehen.

Die Rolle der Bundeswehr in der Cyber-Abwehr könnte künftig gestärkt werden. So schreibt der Präsident des Cyber-Sicherheitsrats Deutschland, Hans-Wilhelm Dünn: „Mit unserer Solidarität für die Ukraine wird auch Deutschland zum Ziel russischer Aggressionen, sei es durch Sanktionen oder Cyberattacken. Die Bundeswehr als Verteidigungsarmee muss in die Lage versetzt werden, das Land an seinen verwundbarsten Punkten zu schützen: in der kritischen Infrastruktur mit Energieversorgern, Krankenhäusern, Transportunternehmen, Banken, Medien und Kommunikationsnetzen."

## Verpflichtung zum IT-Selbstschutz

Zunächst aber sind diese Einrichtungen und Unternehmen dazu verpflichtet, selbst ihre ITSicherheit zu gewährleisten. Das BSI steht ihnen dabei beratend zur Seite. Man habe seinen Eigenschutz und seine Krisenreaktion gestärkt und hat dazu das Nationale ITKrisenreaktionszentrum aktiviert, sagte ein BSI-Sprecher dem „RND". Außerdem seien die Bundesverwaltung, Betreiber kritischer Infrastrukturen und weitere Organisationen und Unternehmen sensibilisiert und zu einer erhöhten Wachsamkeit und Reaktionsbereitschaft aufgerufen worden.

Ob deutsche Behörden, Versorger oder andere systemkritische Einrichtungen und Unternehmen ausreichend vor Cyberattacken geschützt sind, gilt als fragwürdig. Im Oktober vergangenen Jahres

schrieb der Branchenverband Bitkom zum BSI-Lagebericht 2021, 86 Prozent der deutschen Unternehmen seien zuletzt durch Cyberangriffe geschädigt worden. Eine Recherche des BR und von „Zeit Online“ ergab vergangenen Sommer, dass in den vergangenen sechs Jahren mindestens 100 deutsche Ämter, Regierungsstellen, landeseigene Kliniken, Stadtverwaltungen und Gerichte Opfer von Hackerangriffen wurden.

## Noch viel Luft nach oben

Man kann davon ausgehen, dass KRITIS und UBI besser geschützt sind, allerdings verpflichten sie BSI-Gesetz oder Energiewirtschaftsgesetz nur zu Mindestanforderungen. Zwar müssen sie Störungen melden. Aus der Antwort der Bundesregierung auf eine kleine Anfrage der FDP-Fraktion ging im vergangenen Jahr aber hervor, dass beispielsweise Netzbetreiber keine expliziten Meldungen zu Cyberangriffen machen müssen. Man weiß also nicht, ob eine Störung ein Fehler oder eine Hackerattacke war.

Manches Unternehmen scheint auch seine Verpflichtung zur IT-Sicherheit nicht so ernst zu nehmen, wie es vorgeschrieben ist. So haben sich die Berliner Verkehrsbetriebe (BVG) laut „Tagesspiegel“ nach jahrelanger Weigerung erst unter massivem politischen Druck bereit erklärt, im vollen Umfang mit dem BSI zu kooperieren.

## Hackerangriffe benötigen Vorbereitung und Ressourcen

Hackerangriffe auf gut abgesicherte Ziele sind nicht von heute auf morgen möglich, sondern sind aufwändig und benötigen Vorbereitung. Zunächst benötige man kompetentes Personal, das auf dem Stand der Technik ist, sagt Matthias Schulze von der Stiftung Wissenschaft und Politik (SWP) in Berlin. Dazu kommt die Infrastruktur, zum Beispiel Botnetze und Commandand- Control-Server.

Systeme müssten gescannt, Schad-Software geschrieben oder vorher auch noch eine bisher unbekannte Schwachstelle entwickelt werden. Dann müsse die Schad-Software noch ins Ziel geführt werden, beispielsweise mit Phishing, so Schulze. Das klappe dann vielleicht nicht oder die Schad-Software funktioniere möglicherweise nicht wie geplant und müsse nachjustiert werden. Anschließend müssten die Hacker das System ausspähen „und erst ganz am Ende der Kette kann ich einen Effekt auslösen, also Daten löschen, Daten verschlüsseln oder ein physisches System stören, das vielleicht dranhängt.“

## Warum sieht man noch nichts?

Trotzdem wundert sich der Sicherheitsforscher, „dass man bisher noch nichts gesehen hat.“ Dafür gäbe es mehrere mögliche Erklärungen, sagt er. Eventuell sehe man gar nicht, was vorgehe, vielleicht wurden Angriffe schon erfolgreich abgewehrt. Es könne aber auch sein, dass Putins Hacker nichts von seinen Plänen wussten, es gäbe ja Berichte, russische Einheiten im Feld seien von einer Übung ausgegangen.

Der russische Staat sei schließlich paranoid und teile Nachrichten und Informationen ungern. Auch die Nachrichtendienste, die die Cyber-Einheiten beherbergten, seien sich nicht grün und stünden im Wettbewerb zueinander. Das sei aber reine Spekulation, betont Schulze.

Es sei auch möglich, dass die Hacker schon Zugänge zu Systemen hätten, sie aber noch nicht eingesetzt wurden, weil Putin noch zögere, in westlichen Ländern kritische Infrastruktur anzugreifen. „Vielleicht haben sie auch keine Zugänge oder die Verteidigung war erfolgreich.“

## Gefährliche Kaskadeneffekte

Entwarnung kann der Berliner Sicherheitsforscher aber nicht geben. Er glaube zwar, dass Putin die Geschlossenheit der NATO sehe und ein Cyberangriff auf Westeuropa im Sinne eines konventionellen

Angriffs interpretiert werden könnte. „Andererseits sind wir ja schon im nuklearen Säbelrasseln und damit in der Eskalationsdynamik bereits weiter“, so Schulze.

Gegenwärtig geht er davon aus, dass man sich auf einen längerfristigen Konflikt mit Moskau einstellen müsse. Russische Cyberangriffe würden künftig auf der Tagesordnung sein, beispielsweise um strategische Vorteile zu erlangen oder um die Europäische Union zu schwächen.

Schulze befürchtet, dass es dabei zu sogenannten Kaskadeneffekten kommen könnte – auch aus scheinbar banalen Ereignissen. So könne es passieren, dass beispielsweise ein Server, der die Uhrzeit von Systemen steuert, bei einem Angriff in Mitleidenschaft gezogen wird. Als Folge könne irgendwo am anderen Ende des Internets „irgendetwas Dummes passieren.“

## Sehr riskanter Hacktivisten-Einsatz

Dem Sicherheitsforscher bereiten derzeit auch weniger „offizielle“ Cyberangriffe Sorgen. Für die Ukraine griffen eine IT-Armee aus Freiwilligen und die selbsternannten belarussischen Cyper-Partisanen wahllos russische Ziele an. An die Seite Putins habe sich unter anderem die kriminelle Ransomware-Gruppe „Conti“ gestellt. Wenn diese Hacker sich jetzt gegenseitig beharkten, „wird das auch unschön.“

Schulze rät deutschen Hacktivisten dringend davon ab, sich daran zu beteiligen. Es könne zu einer unkontrollierbaren Eskalation führen, und wenn die Spur einer Cyberattacke in die Bundesrepublik führe, werde dies höchstwahrscheinlich von russischer Seite als eine vom Westen konzertierte Aktion interpretiert. „Das sehe ich sehr, sehr kritisch.“

*Montag, 1. März 2022*

***600 IT-Fachkräfte fehlen***

# Deutschland ungenügend gegen „Cyberkrieg“ gewappnet

## 3600 IT-Spezialisten sollen deutsche Ministerien und Behörden vor möglichen Cyberangriffen schützen. Allerdings sind derzeit 600 dieser Stellen unbesetzt. Angesichts eines drohenden „Cyberkrieges“ durch Russland sei das fatal, kritisiert die Linke-Digitalexpertin Domscheit-Berg.

Bei Bundesministerien und -behörden ist jede sechste Stelle für IT-Sicherheit im Kampf gegen Cyberangriffe unbesetzt. Nach einer Antwort der Bundesregierung auf eine Anfrage der Linksfraktion fehlen derzeit 600 Fachkräfte für die 3600 Stellen für IT-Sicherheit im Bereich der verschiedenen Bundesministerien, wie die „Augsburger Allgemeine“ berichtet. Im Bereich des Bundesinnenministeriums, zu dem das Bundesamt für Sicherheit in der Informationstechnik (BSI) gehört, sei sogar jede fünfte Stelle unbesetzt.

Die Linke-Digitalexpertin Anke Domscheit-Berg kritisierte die mangelnde Personalausstattung als Gefahr vor dem Hintergrund des russischen Angriffs auf die Ukraine. „Dieser erste völlig offen ausgetragene Cyberkrieg hat eine völlig neue Dimension erreicht“, sagte Domscheit-Berg der Zeitung. „Ich fürchte, er wird nicht begrenzt sein auf ukrainische und russische Einrichtungen.“

### „Cyberkrieg“ „offensichtlich länger vorbereitet“

Die russische Seite habe den „Cyberkrieg“ „offensichtlich länger vorbereitet“, sagte die Linken-Politikerin. Dabei werde Schadsoftware eingeschleust und über längere Zeit zum Ausspionieren der IT-Systeme und ihrer Daten genutzt, aber erst für spätere Angriffe weiter aktiviert. Auch in Deutschland habe es bereits derartige Attacken gegeben.

„Die Bedrohung ist real und ich kann nicht verstehen, dass die Bundesregierung das Thema nicht höher priorisiert“, sagte die Bundestagsabgeordnete. „Die Gefahr durch Cyberangriffe steigt von Jahr zu Jahr, immer wieder veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik neue Rekordzahlen zu digitalen Angriffen.“

Täglich gebe es über 300.000 neue Schadsoftware-Varianten, warnte Domscheit-Berg. Ransomware-Angriffe, bei denen Systeme lahmgelegt werden, um Geld zu erpressen, seien „dabei die größte Bedrohung“. In Deutschland seien damit bereits „Krankenhäuser, Universitäten, Kommunen und ganze Landkreise lahmgelegt“ worden.

*Dienstag, 18. Januar 2022*

***„Risikobarometer" der Allianz***

# Konzerne haben große Angst vor Cyberattacken

## Angriffe auf die IT-Infrastruktur sind die größte Sorge von Managern weltweit. Cyberattacken hatten im vergangenen Jahr für Schäden in Billionenhöhe gesorgt. Tendenz: steigend. In deutschen Unternehmen ist die Angst vor einem anderen Vorfall noch größer. Sogar in Pandemiezeiten.

Manager und Sicherheitsfachleute weltweit sehen in Cyberangriffen die größte Gefahr für Unternehmen. Im „Risikobarometer" des zur Allianz gehörenden Industrieversicherers AGCS liegen kriminelle Hacker mit ihren Aktivitäten auf Rang eins.

Betriebsunterbrechungen, Naturkatastrophen und Pandemien folgen auf den Plätzen zwei bis vier. Das Unternehmen hat im vergangenen Herbst insgesamt 2650 Fachleute in 89 Ländern befragt. Dazu zählten über 1200 Führungskräfte großer Unternehmen mit mehr als 500 Millionen Dollar Jahresumsatz. An der Umfrage nahmen auch eigene Fachleute der Allianz teil. Bei den 351 Teilnehmern in Deutschland waren die ersten beiden Plätze vertauscht: Betriebsunterbrechung kam vor Cyberangriffen auf Platz eins.

Die zwei Hauptgefahren Cyberangriffe und Betriebsunterbrechung hängen jedoch in vielen Fällen zusammen, wie AGCS-Manager Jens Krickhahn erläuterte. Sehr stark zugenommen hat in den vergangenen Jahren die Zahl der „Ransomware"-Attacken. Mithilfe von bösartiger Verschlüsselungssoftware legen Hacker Computernetze lahm, um anschließend für die Entsperrung hohe Summen zu erpressen. Auch sehr gute IT-Sicherheitsvorkehrungen schützen nicht hundertprozentig gegen Hackerangriffe: „Die Unternehmen stecken sehr viel Geld in die Weiterentwicklung der IT-Sicherheit, aber dennoch stellen wir fest, dass Angreifer durchkommen und Unternehmen zum Teil auch enorm schädigen können", sagte Krickhahn.

### Gewaltiger Schaden mit steigender Tendenz

Die Einschätzung der von der Allianz befragten Experten deckt sich mit anderen Analysen zum Thema Cyberkriminalität. So schätzt das in der IT-Branche häufig zitierte USUnternehmen Cybersecurity Ventures, dass die durch Cyberkriminalität verursachten weltweiten Schäden 2021 sechs Billionen Dollar erreicht haben. Bis 2025 könnte diese Summe demnach auf 10,5 Billionen Dollar steigen. Die immense Summe beinhaltet Datendiebstahl und -zerstörung, Finanzkriminalität, Produktivitätsverluste, Diebstahl geistigen Eigentums und andere Delikte ebenso wie die Kosten der Schadenbeseitigung.

Mitte des Jahrzehnts wären dies dann höhere Gewinne als im weltweiten Drogenhandel und eine höhere Summe als die Bruttoinlandsprodukte sämtlicher Staaten mit Ausnahme der USA und Chinas, heißt es in einer zum Jahreswechsel veröffentlichten Einschätzung des US-Unternehmens zu den Trends im kriminellen Cyberbusiness.

„Kein Unternehmen und keine Behörde ist in der heutigen Zeit vor Cyberangriffen sicher", sagt Sebastian Artz, Bereichsleiter Cyber- und Informationssicherheit beim ITBranchenverband Bitkom. „Deshalb ist es entscheidend, sich für den Ernstfall zu wappnen und sich mit dem Thema Cybersicherheit proaktiv auseinanderzusetzen. Vor allem das Thema Ransomware wird in 2022 weiter Hochkonjunktur haben." Denn unter den verschiedenen Formen der Cyberkriminalität ist Erpressung das am schnellsten wachsende Delikt. 2021 haben kriminelle Banden nach Schätzung von Cybersecurity Ventures auf diese Weise weltweit 20 Milliarden Dollar erlöst.

*Dienstag, 18. Januar 2022*

***Bedrohung „für uns alle“***

# Europol zerschlägt Netzwerk von Cyberverbrechern

## Ein Angriff auf die Verwaltung einer niedersächsischen Kleinstadt löst internationale Ermittlungen gegen ein Netz aus Cyberkriminellen aus. Diese nutzen einen Onlinedienst, um ihre Opfer zu erpressen. Nun können die Behörden einen großen Erfolg verbuchen.

Europäische Ermittler haben ein Netzwerk von Cyberkriminellen unschädlich gemacht und damit Schäden in Millionenhöhe verhindert. In zehn Ländern seien 15 Server ausgeschaltet worden, die die Anonymität von Kriminellen im Internet gesichert hätten, teilte die europäische Polizeibehörde Europol in Den Haag mit. Ausgangspunkt der zweijährigen Ermittlungen war ein Cyberangriff auf die Stadtverwaltung von Neustadt am Rübenberge von 2019 – nach Angaben der federführenden Polizeidirektion Hannover. Weltweit seien verschiedene Behörden beteiligt gewesen.

Laut Europol nutzten Kriminelle die Infrastruktur des Dienstes VPNLab.net für schwere Cyber-Verbrechen. VPN („virtual private network“ oder „virtuelles privates Netzwerk“) bietet Nutzern die Möglichkeit, anonym miteinander zu kommunizieren – ohne dass Außenstehende Einblick haben. Kriminelle nutzen den Service auch für den abgesicherten Zugang zum Internet.

Die Aktion fand bereits am Montag statt. Beteiligt waren neben der Polizeidirektion Hannover und der Staatsanwaltschaft Verden unter anderem Europol und die europäische Justizbehörde Eurojust, die Kontakt zu Ermittlern etwa aus den Niederlanden, Kanada, der Tschechischen Republik, Frankreich, Ungarn, Lettland und der Ukraine herstellte. Außerdem waren das FBI in den USA sowie Ermittler in Großbritannien beteiligt.

### Angriff legt Verwaltung lahm

Zu den bekannten Opfern von Cyberkriminalität zählte 2019 die Stadtverwaltung von Neustadt am Rübenberge in der Region Hannover, wo Elterngeldanträge, Baupläne und vieles mehr verschlüsselt wurden. Die Verwaltung der rund 45.000 Einwohner zählenden Stadt konnte einzelne Dienstleistungen bis ins erste Quartal 2020 daher nicht anbieten.

Neben Kommunen sind auch Unternehmen betroffen. Das Ziel der Kriminellen: Gegen Lösegeld werden die Daten wieder freigegeben. Niedersachsens Innenminister Boris Pistorius sagte, der sogenannte „Takedown“ des Netzwerks zeige, „dass wir als Sicherheitsbehörden dazu in der Lage sind, schwerkriminellen Cyber-Netzwerken das Handwerk zu legen“. Der SPD-Politiker betonte: „Das schärfste Schwert gegen international agierende Verbrecher ist ein gemeinsames und eng abgestimmtes Vorgehen.“

Niedersachsens Justizministerin Barbara Havliza erklärte, Cyberangriffe seien eine reale Bedrohung – „für uns alle“. Die CDU-Politikerin sagte: „Ist die Schadsoftware erstmal im System, sind die Folgen oft katastrophal. Die Lösegeldforderungen gehen in die Millionen, der Verlust sensibler Daten kann einen riesigen Schaden verursachen.“

### VPN-Anbieter im Visier

VPNLab.net bestand nach Angaben von Europol seit 2008. Der Dienst war „besonders populär bei

Cyber-Kriminellen“, wie Europol mitteilte. Der Grund: er bot auch ein doppeltes VPN mit Servern in mehreren Ländern an. Damit hätten die Dienste genutzt werden können, um Verbrechen zu begehen – ohne Angst, von den Behörden entdeckt zu werden. Laut Polizeidirektion Hannover werden VPN-Dienste von vielen Anbietern weltweit angeboten und auch für legale Zwecke genutzt, um sich vor Nachverfolgung zu schützen.

Der Provider war bei der Aufklärung verschiedener Fälle ins Visier der Ermittler geraten. Europol schätzt, dass schwere Cyber-Attacken verhindert werden konnten. Bei der über die Server verschickte Schadsoftware handele es sich um „Ryuk“ – eine Software, die von kriminellen Vereinigungen genutzt werde, um Behörden, Firmen und Einrichtungen zu attackieren und Lösegeld zu erpressen, teilte die Polizei mit. Bei Angriffen mit dieser Schadsoftware verursachten die Täter immer wieder Schäden in Millionenhöhe.

## Programm verschlüsselt Daten

Bei „Ryuk“ handelt es sich laut Polizei um sogenannte „Ransomware“ („ransom“ bedeutet Lösegeld, „ware“ ist die Abkürzung für Software). Gelangt das Programm auf einen Computer oder ein Netzwerk, verschlüsselt es Fotos, Videos, Dokumente oder ganze Datenbanken. Auf dem Endgerät wird eine Text-Datei mit einer Lösegeldforderung hinterlassen. Systemkopien werden demnach ebenfalls verschlüsselt oder gelöscht.

Die Schadsoftware zu entfernen oder das System auf einen Zeitpunkt vor dem Angriff zurückzusetzen, führt dazu, dass auch bei einer Zahlung die Dateien nicht entschlüsselt werden können. Dringt die Software in ein Netzwerk ein, kann sie nach Polizeiangaben ausgeschaltete Rechner per WLAN-Verbindung einschalten, um sie zu infizieren. Der Angriff erfolge meist per Phishing-Mail – eine E-Mail mit einem Link oder einer Datei im Anhang.

„Ryuk“ werde auch als Service angeboten – eine kriminelle Gruppe biete es einer anderen an und werde prozentual an der erpressten Beute beteiligt. Pistorius, Mitglied im Kontrollgremium von Europol, forderte erneut den Ausbau der Kompetenzen und Mittel der Behörde: „Täter agieren längst höchst dynamisch und grenzüberschreitend. Die Antwort kann nur eine starke europäische Behörde im Netzwerk der europäischen Sicherheitsbehörden sein.“

*Sonntag, 12. Dezember 2021*

### *Von Log4j-Lücke betroffen*

# Mehrere Behörden anfällig für Hacker-Angriffe

## Beim BSI herrscht Alarmstufe Rot, seit die Log4j-Sicherheitslücke bekannt ist. Einem Bericht zufolge ist nun auch klar, dass mehrere Stellen der Bundesverwaltung potenzielles Einfallstor für Hacker-Attacken war – nach allem, was bisher bekannt ist, jedoch ohne Folgen.

Einem Bericht zufolge waren mehrere Stellen in der Bundesverwaltung wegen der schwerwiegenden Sicherheitslücke für Cyber-Angriffe verwundbar. Das haben laut „Spiegel" Überprüfungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) ergeben. Hintergrund ist die für Hackerangriffe anfällige Programmbibliothek Log4j, die bei einer einstelligen Zahl an Bundesbehörden zum Einsatz kommt.

„Bei einer Schwachstelle mit dieser Verbreitung ist auch die Bundesverwaltung betroffen", heißt es aus dem BSI. Der Behörde seien einzelne verwundbare Systeme bekannt und man habe bereits entsprechende Schutzmaßnahmen eingeleitet. Bisher liegen keinerlei Hinweise vor, dass die Schwachstelle in der Bundesverwaltung tatsächlich ausgenutzt wurde. Zumindest in einigen Fällen konnte das BSI nachvollziehen, dass die Probleme bereits behoben wurden.

Hacker können durch die Schwachstelle theoretisch eigene Schadsoftware nachladen und so Daten stehlen. Seit Freitag warnen IT-Fachleute in aller Welt, weil es sich bei Log4j um eine äußerst weitverbreitete Programmbibliothek handelt.

Am Samstag hatte das BSI die höchste, rote Warnstufe wegen der Sicherheitslücke ausgerufen. Gleichzeitig wurde laut „Spiegel" auch das IT-Krisenreaktionszentrum der Behörde aktiviert. Dabei handelt es sich um ein aufgestocktes Lagezentrum, in dem seitdem rund um die Uhr mehrere Personen mit dem Problem befasst sind.

Im nationalen Cyberabwehrzentrum ist die Schwachstelle ebenfalls thematisiert worden. Das Innenministerium sei dem Bericht zufolge mehrfach über die aktuellen Vorgänge unterrichtet worden, auch weil das Thema auf der Bundespressekonferenz am Montag eine Rolle spielen könnte. Außerdem habe eine einstellige Anzahl an Unternehmen aus dem Bereich Kritische Infrastruktur dem BSI gemeldet, dass sie von der Schwachstelle betroffen seien.

*Donnerstag, 28. Oktober 2021*

***Spur führt nach Russland***

# Drahtzieher von Cyber-Erpressung enttarnt

## Das Geschäft mit Erpressungssoftware boomt weltweit. Cyberkriminelle legen die Systeme großer Konzerne lahm und fordern zur Freigabe sensibler Daten ein hohes Lösegeld. Nun machen deutsche Ermittler einen dicken Fisch der berüchtigten Revil-Gruppe aus. Festnehmen können sie ihn jedoch nicht.

Strafverfolger des Landeskriminalamts Baden-Württemberg haben laut Informationen des Bayerischen Rundfunks (BR) und der „Zeit" einen mutmaßlichen Drahtzieher hinter der Schadsoftware Revil ermittelt. Bei der Software handelt es sich den Berichten zufolge um eines der berüchtigtsten Programme für Ransomware-Angriffe. In Deutschland seien unter anderem das Staatstheater Stuttgart, mehrere mittelständische Unternehmen und auch Krankenhäuser davon betroffen.

Bei Ransomware – auch als Erpressungstrojaner bekannt – handelt es sich um eingeschleuste Software, die Computer und andere Systeme blockiert. Anschließend werden die Betreiber erpresst, damit die Systeme wieder freigeschaltet werden. In dem Begriff steckt das englische Wort für Lösegeld („ransom").

Bei dem Tatverdächtigen soll es sich um einen russischen Staatsbürger handeln, der in einer Großstadt im Süden des Landes lebt. Er soll nach Ansicht der Ermittler „zweifelsfrei" der Kerngruppe von Revil und deren mutmaßlichem Vorgänger Gandcrab angehören. Reporter des BR und der „Zeit" hätten Anhaltspunkte dafür gefunden, dass der Verdächtige Geld erhalten habe, das direkt aus Ransomware-Fällen stammen soll.

### Ermittler können Verdächtigen nicht festnehmen

Weder die ermittelnden Behörden – das Bundeskriminalamt und das Landeskriminalamt Baden-Württemberg – noch die Staatsanwaltschaft Stuttgart wollten sich auf Nachfrage der Medien dazu äußern. Auch der Tatverdächtige habe nicht auf Anfragen reagiert. In den Online-Netzwerken habe sich der Mann als Händler von Kryptowährungen mit luxuriösem Lebensstil präsentiert, etwa mit teuren Sportwagen, Designerkleidung und Luxusreisen. Solange er sich in Russland aufhält, könne er allerdings nicht von deutschen Strafverfolgern festgenommen werden.

Mit Ransomware wurden allein in den USA im ersten Halbjahr 2021 590 Millionen US-Dollar (rund 510 Millionen Euro) erpresst. Das geht aus einem aktuellen Bericht der US-Behörde zur Verfolgung von Finanzkriminalität hervor. Die wachsende Bedrohung durch Cyberkriminalität wird in dem Bericht betont.

Die Erpresser lassen sich meistens mit der Kryptowährung Bitcoin bezahlen. Die Auswertungen zeigen 68 verschiedene Varianten von Ransomware. Am verbreitetsten waren in den ersten Monaten dieses Jahres Revil/Sodinokibi, Conti, Darkside, Avaddon und Phobos.

*Donnerstag, 21. Oktober 2021*

***Bericht sieht „Alarmstufe Rot“***

# Profi-Hacker gehen immer aggressiver vor

## Mit immer dreisteren Methoden versuchen Hacker, über das Internet Geld von ihren Opfern zu erbeuten. Der aktuelle Lagebericht zur Cybersicherheit erkennt einen dringenden Handlungsbedarf seitens der Politik. Doch an konkreten Plänen scheint es noch zu mangeln.

Die Bedrohung durch Cyberangriffe ist in Deutschland deutlich gewachsen. Das geht aus dem Lagebericht 2021 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hervor, der nun veröffentlicht wurde. Darin wird die aktuelle Situation als „angespannt bis kritisch“ eingeschätzt. Ein Jahr zuvor hatte die Bonner Behörde die Lage noch als „angespannt“ charakterisiert. In Teilbereichen herrsche schon „Alarmstufe Rot“, sagt BSIPräsident Arne Schönbohm.

Ursächlich dafür seien die deutliche Professionalisierung der Cyberkriminellen, die zunehmende digitale Vernetzung und die Verbreitung gravierender Schwachstellen in ITProdukten. „Informationssicherheit muss einen deutlich höheren Stellenwert einnehmen und zur Grundlage aller Digitalisierungsprojekte werden“, heißt es in dem Bericht. Das klingt schlüssig. Aber sind die Bundesregierung und ihre Behörden dafür richtig aufgestellt?

Auf die Frage, ob es künftig ein Bundesdigitalministerium geben sollte, will der scheidende Bundesinnenminister Horst Seehofer, dessen Haus bislang die Verantwortung für das BSI und die Digitalisierung der Verwaltung trägt, nicht direkt antworten. An die Adresse der künftigen Koalitionäre sagt er nur, man werde „die allgemeine Sicherheit von der Cybersicherheit nicht trennen können“.

### Perfide Methoden

Nach Einschätzung des BSI nutzen Kriminelle inzwischen teilweise sehr aufwendige, mehrstufige Angriffsstrategien, die früher nur in der Cyberspionage zur Anwendung kamen. Eine Methode: Während ein krimineller Hacker mit seinem Opfer über ein Lösegeld für den Zugriff auf von ihm verschlüsselte Daten verhandelt, startet er gleichzeitig einen Überlastungsangriff auf ein Ausweichsystem, das der Geschädigte nutzt, um seine Geschäftstätigkeit fortzusetzen. Oder der Täter veröffentlicht auf sogenannten Leak-Seiten erbeutete Daten, um das Opfer noch mehr unter Druck zu setzen.

Einige Angreifer gehen demnach auch auf Kunden oder Partner des Opfers zu, um den Druck zu erhöhen. Als Beispiel nennt das BSI in seinem Bericht den Fall einer psychotherapeutischen Praxis, wo nicht nur die Praxisinhaber, sondern auch deren Patientinnen und Patienten erpresst worden waren. Die Behörde ermahnt in diesem Zusammenhang alle Betroffenen, Angriffe möglichst schnell zu melden, um weiteren Schaden zu vermeiden.

### Millionen verschiedene Schadprogramme

Die Zahl der registrierten neuen Varianten von Schadprogrammen lag mit 144 Millionen laut BSI um 22 Prozent über dem Wert im zurückliegenden Berichtszeitraum. Im Februar 2021 wurden nach Angaben des Bundesamtes an einem Tag 553.000 Schadprogrammvarianten entdeckt – ein neuer Spitzenwert. Zwischen Januar und Mai wurde dem Bericht zufolge eine große Zahl von Attacken registriert, bei denen Erpresser vorgaben, über Videomaterial des Opfers zu verfügen, das dieses angeblich beim Besuch einer Webseite mit pornografischen Inhalten zeige. Die Drohung: Sollte das

Opfer nicht einen vierstelligen Euro-Betrag in Bitcoin zahlen, werde das kompromittierende Video an alle Kontakte des Opfers verschickt.

„Die Schäden durch Erpressung, verbunden mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen, sind seit 2019 um 358 Prozent gestiegen“, sagt Susanne Dehmel, Mitglied der Geschäftsleitung des Branchenverbandes Bitkom. Damit sich Unternehmen und auch Privatpersonen besser schützen können, sollte es ihrer Ansicht nach für alle die Möglichkeit geben, sich über die aktuelle Cyber-Bedrohungslage zu informieren. „Dazu müssen wir Echtzeit-Informationen nutzen und EU-weit in einem zentralen Dashboard sammeln – ähnlich dem Corona-Dashboard des Robert-Koch-Instituts.“

*Dienstag, 24. August 2021*

***„Cyber Security Report 2021“***

# Studie ergibt steigende Sorgen um Cybersicherheit

## Top-Manager und Politiker in Deutschland sehen die Bedrohungslage im Cyberraum auf einem Rekordniveau. Neben klassischen Hacker-Angriffen und Datendiebstählen fürchten sich die Entscheidungsträger vor allem vor einer Meinungsmanipulation durch gefälschte oder unrichtige Nachrichten. Das geht aus dem „Cyber Security Report 2021“ hervor, der am Dienstag von dem Meinungsforschungsinstitut Allensbach und dem Wirtschaftsprüfungsunternehmen Deloitte in Berlin veröffentlicht wurde.

Danach sehen 77 Prozent der Abgeordneten und Führungskräfte den Datenbetrug als höchstes Cyberrisiko für die Menschen in Deutschland an. Vor zwei Jahren lag dieser Wert bei 70 Prozent.

Auf ein neues Rekordhoch stieg auch die Sorge vor Fake News: 75 Prozent der Befragten sehen ein Risiko, dass die öffentliche Meinung durch gefälschte oder unrichtige Nachrichten manipuliert wird. Beschleunigt durch die Corona-Pandemie verlagere sich der Wahlkampf teilweise ins Netz. Entsprechend groß sei die Sorge um die Manipulation der öffentlichen Meinung durch Fake News.

„Information, Meinungsbildung und gesellschaftliche Debatten verändern sich durch die Digitalisierung und damit auch die demokratische Kultur“, erklärte Prof. Renate Köcher, Geschäftsführerin des Instituts für Demoskopie Allensbach. „Das bietet Chancen, bringt aber auch erhebliche Risiken mit sich, gerade auch für die Meinungsbildung vor Wahlen.“

Acht Jahre nach den Enthüllungen des US-Whistleblowers Edward Snowden, der ein weitreichendes Überwachungsprogramm durch US-amerikanische und britische Geheimdienste aufgedeckt hat, geht die Sorge der Entscheidungsträger vor einer staatlichen Überwachung zurück. Aktuell fürchten sich noch 48 Prozent der Befragten vor einer Überwachung aus Ländern wie den USA oder China. 2017 lag dieser Wert noch bei 54 Prozent. Eine Überwachung durch den deutschen Staat befürchten aktuell neun Prozent, 2017 befürchteten noch 21 Prozent eine Bespitzelung im Inland.

*Montag, 31. Mai 2021*

***Studie***

# Nutzer sozialer Medien anfälliger für Cyber-Angriffe

## Nutzer von sozialen Netzwerken sind deutlich anfälliger für Attacken von Cyberkriminellen als Menschen, die nicht auf Plattformen wie Facebook angemeldet sind.

Wie aus einer am Montag veröffentlichten Studie der Technischen Universität Darmstadt und eines Startups für IT-Sicherheit hervorging, erstellen Kriminelle personalisierte Betrugsmails oftmals anhand frei zugänglicher Informationen ihrer Opfer. Dazu zählten etwa Angaben zum aktuellen Job, der Ausbildung, Hobbys oder Kollegen.

Die in den Phishingmails enthaltenen zutreffenden Angaben würden die Opfer dazu verleiten, gesicherte Informationen wie Passwörter zu verraten oder auf nicht vertrauenswürdige Links zu klicken. Dabei würden dann schlimmstenfalls Schadsoftwares wie Trojaner heruntergeladen.

„Nutzerinnen und Nutzer von sozialen Medien sind als Hochrisikogruppen bezüglich Phishingangriffen anzusehen“, erklärte Anjuli Franz, Mitautorin der Studie. Einerseits gäben Social-Media-Nutzer online mehr über sich preis als andere. Andererseits reagierten sie aus Gewohnheit „direkt und automatisiert“ auf Aufforderungen und Hinweise.

Im Zuge der im April bekannt gewordenen Datenleaks bei Linkedin und Facebook seien Cyberkriminellen Daten einer großen Zahl von Nutzern „auf dem Silbertablett serviert“ worden. Nutzer sozialer Medien und Unternehmen müssten sich in den kommenden Monaten auf „besonders gemeine und gezielte Phishingangriffe“ einstellen, hieß es weiter.

*Donnerstag, 20. Mai 2021*

***„Ist mir nicht leichtgefallen“***

# Pipeline-Chef räumt Lösegeldzahlung ein

## Der US-Pipeline-Betreiber Colonial hat die Zahlung von 4,4 Millionen Dollar in Bitcoin an Erpresser eingeräumt, obwohl Behörden dringend von Lösegeldzahlungen abraten. Die Entscheidung sei „hochkontrovers“, aber „das Richtige für das Land“ gewesen, sagt CEO Blount.

Der Betreiber der größten US-Benzin-Pipeline Colonial hat erstmals öffentlich eine millionenschwere Lösegeldzahlung an Computer-Hacker eingeräumt. Er habe die Zahlung in Höhe von 4,4 Millionen Dollar autorisiert, sagte Colonial-Chef Joseph Blount dem „Wall Street Journal“. „Ich weiß, dass es eine hochkontroverse Entscheidung war.“

Doch das Unternehmen sei sich über das Ausmaß der verursachten Systemschäden unsicher gewesen und habe nicht einschätzen können, wie lange es dauern würde, bis die Pipeline wieder ans Netz gehen könne. Die Lösegeldzahlung sei deshalb im Interesse des Landes richtig gewesen. „Es ist mir nicht leichtgefallen“, erklärte Blount weiter.

Colonial war Ziel eines Hacker-Angriffs geworden und hatte den Betrieb der Pipeline, durch die etwa 45 Prozent aller an der US-Ostküste verbrauchten Kraftstoffe laufen, deshalb zeitweise komplett eingestellt. In Teilen der USA kam es darum in der vergangenen Woche zu Benzinengpässen und mitunter auch zu Turbulenzen an Tankstellen. Inzwischen läuft die Pipeline laut Colonial aber wieder.

### Behörden warnen vor Anreizen für Erpressungen

Die Lösegeldzahlung erfolgte nach Informationen des „Wall Street Journal“ am 7. Mai in der Digitalwährung Bitcoin. Die im Gegenzug von den Hackern bereitgestellten Entschlüsselungs-Tools hätten jedoch nicht ausgereicht, um das System wieder voll herzustellen. US-Behörden raten Unternehmen dringend davon ab, Lösegeld zu zahlen, um Cyber-Kriminellen keine Anreize für Erpressungen zu bieten.

So entschied sich beispielsweise Irland bisher, im aktuellen Ransomware-Befall seiner Gesundheits-IT den Forderungen nicht nachzugeben. Der Fall von Colonial Pipeline hatte dazu geführt, dass die Erpresser der sogenannten Darkside-Gruppe sich für die sozialen Folgen des Angriffs entschuldigten. Sie hätten Geld verdienen und keine gesellschaftlichen Probleme auslösen wollen, schrieben die Erpresser, nachdem es etwa zu Benzin- Hamsterkäufen an Tankstellen kam. Was die tatsächliche Motivation hinter der Entschuldigung war, ist schwer abzuschätzen.

Etwa eine Woche nach dem bekanntgewordenen Angriff gab mutmaßlich Darkside selbst bekannt, dass die Gruppe Zugriff auf ihre erbeuteten Bitcoins und ihre Blog-Infrastruktur verloren habe. Aufgrund des Drucks aus den USA werde die Gruppe ihre Operationen einstellen. Ob das tatsächlich der Fall ist oder ob die Gruppe künftig unter anderem Namen wiederkehren könnte, ist unklar.

*Montag, 3. Mai 2021*

***White-Hat-Hackerangriffe im produzierenden Gewerbe***

# „Wir waren Gott in den IT-Systemen“

## Lassen sich kleine und mittelständische Betriebe im produzierenden Gewerbe von einem Hacker knacken? Der IT-Sicherheitsexperte Michael Wiesner hat es für den GDV versucht – und war erschreckend erfolgreich.

Wenn die Maschine die Fertigung selbst organisiert und intelligente Roboter Menschen bei der Fertigung zur Hand gehen, ist das Industrie 4.0. Und intelligente Lieferketten, die Material just in time dahin bringen, wo es benötigt wird, sind im produzierenden Gewerbe zunehmend so selbstverständlich wie intelligente Steuerketten, die wissen, wann sie das nächste Mal gewartet werden müssen. Doch wie gut sind die Maschinendaten vor Hackerangriffen geschützt? Sind Produktionsbetriebe bei der IT-Sicherheit genauso innovativ wie bei der Fertigung?

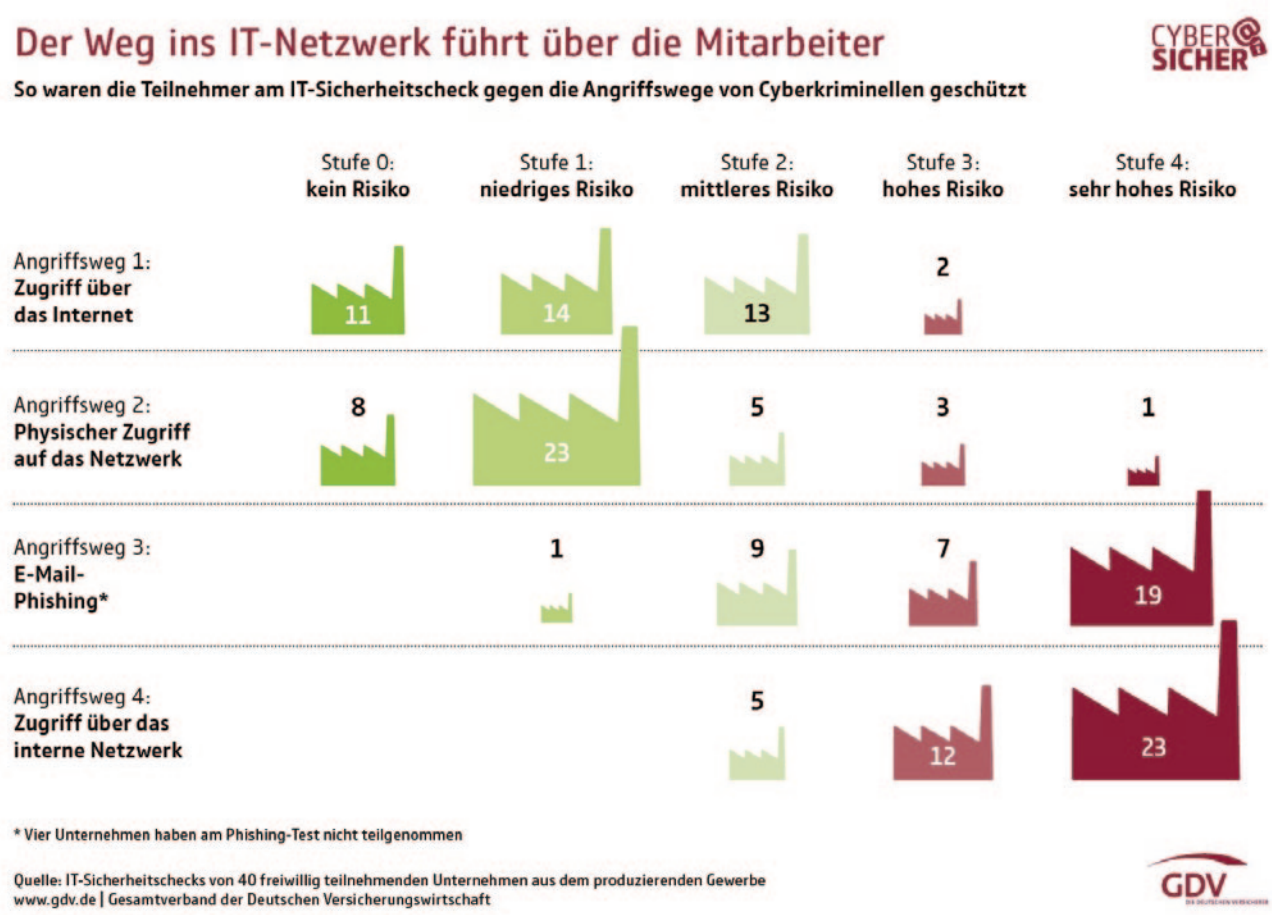
„Sagen wir es mal so: Die Eigenwahrnehmung in puncto Informationssicherheit unterscheidet sich bei sehr vielen Mittelständlern ganz eklatant von der Realität“, sagt Michael Wiesner. Als sogenannter White-Hat-Hacker wird er von Unternehmen beauftragt, um in simulierten Angriffen ihren tatsächlichen Schutz zu prüfen und auf Sicherheitslücken aufmerksam zu machen. Für den Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat er 40 kleine und mittelständische Unternehmen aus dem produzierenden Gewerbe einem mehrstufigen Stresstest unterzogen. „Das Ergebnis war insgesamt nicht schön, aber es hat mich auch nicht überrascht“, berichtet der IT-Sicherheitsexperte.

„Nicht schön” – das bedeutet im Klartext: Bei mehr als der Hälfte der Firmen konnten Wiesner und sein Team die Systeme hacken. Spielend leicht hätten sie Daten manipulieren und Maschinen übernehmen können. Ein verheerendes Fazit – vor allem, weil sich die Unternehmen freiwillig für den Test gemeldet hatten. Sie waren also vorgewarnt und hätten vorbereitet sein können. Dabei verhielten sich die IT-Sicherheitsspezialisten wie echte Cyberkriminelle, wenn sie es auf ein ganz bestimmtes Ziel abgesehen haben: Sie suchen den schnellsten Weg ins Herz der Systeme. Stufe Eins ist zunächst einmal ganz analog. Wie ist der Eingangsbereich des Unternehmens gesichert? Gibt es dort Möglichkeiten, leicht ins Netzwerk oder an Passwörter von Angestellten zu gelangen? In einer zweiten Stufe schickten die Experten Phishing-Mails an die ganze Belegschaft. Waren sie dann erst einmal in ein System eingedrungen, erfolgte der Angriff auf alle möglichen Datenbanken und Maschinensteuerungen der Unternehmen.

### Unternehmen sind Eindringlingen schutzlos ausgeliefert

Die größte Schwachstelle ist noch immer der Mensch. Allein über Phishing-Mails und gefälschte Webseiten gelangte Wiesner an die Zugangsdaten von ZOO Mitarbeiterinnen und Mitarbeitern aus 19 Firmen. In sieben weiteren Unternehmen gaben Angestellte zwar keine Daten preis – dafür klickten sie aber Links an, über die echte Cyberkriminelle leicht Schadsoftware im Firmensystem hätten installieren können. Eigentlich eine alarmierende Bilanz. Aber: „Dass Phishing so erfolgreich war, hat die wenigsten Unternehmen überrascht“, berichtet Wiesner von der Reaktion der Firmen.

Geschockt zeigten sich einige Firmen immerhin über das, was dann folgte. „Wenn wir einmal in ein Netzwerk eingedrungen waren, konnten wir dort machen, was wir wollten – wir waren praktisch Gott in den IT-Systemen“, beschreibt der White-Hat-Hacker. Das heißt: Wenn ein Angreifer einmal drin ist, geben die Systeme auch dann keine Warnung aus, wenn Anomalien auftreten. „Nicht ein Unternehmen verfügte über reaktive Maßnahmen.“




Angesichts solch eklatanter Sicherheitslücken treten die wenigen positiven Ergebnisse der Untersuchung in den Hintergrund. So war die „physische Sicherheit" bei den meisten Mittelständlern weitgehend gegeben. Netzwerk-Stecker in der Lobby oder ähnliche Einfallstore waren überwiegend gut gegen Eindringlinge abgeschirmt. Ebenfalls nur ein kleiner Lichtblick: In einigen Unternehmen gab es getrennte Kreisläufe für unterschiedlich sensible Bereiche. Im Fall eines Hackerangriffs kann das von existentieller Bedeutung sein. Gelingt es Cyberkriminellen etwa sich Zugriff auf den Mailserver zu verschaffen, könnten sie andernfalls nämlich Maschinen kapern und schlimmstenfalls die Produktion komplett stoppen. Allerdings: „Die Segmentierung der Sicherheitskreisläufe verbessert sich nur langsam", sagt IT-Sicherheitsexperte Wiesner. „Inzwischen sehen wir sie immerhin in 20 bis 30 Prozent der Unternehmen."

## Drei zentrale Punkte machen Unternehmen schwach

Insgesamt bemängelt Wiesner die Geschwindigkeit, mit der sich der Sinneswandel in den Unternehmen vollzieht. Für ihn sind es drei zentrale Knackpunkte, die zu den wenig erfreulichen Ergebnissen der Studie führen: unklare Zuständigkeiten, mangelhafte Risikoeinschätzung und fehlende Ressourcen. Wenn es darum geht, wer für die Datensicherheit in der Produktion zuständig ist, schieben sich die Abteilungen nach Erfahrung des Experten die Verantwortung zu häufig gegenseitig zu. Das liege nicht zuletzt an der zunehmenden Digitalisierung der Produktionsprozesse. IT und produktionsnahe Steuerung verschmelzen also immer stärker. „In der Praxis führt das oft zu einem Kompetenzvakuum", erläutert Wiesner. „Die IT fühlt sich nicht für die Maschinensicherheit verantwortlich und die operativen Mitarbeiter fühlen sich nicht als IT-Spezialisten."

Doch sind es längst nicht die Mitarbeitenden, die in mit ihrem Verhalten für die in vielen Betrieben noch immer mangelhafte IT-Sicherheit sorgen. „Dem Management fehlt nach wie vor zu häufig die Expertise, um die richtigen Schritte in der IT-Sicherheit zu gehen", urteilt Wiesner. Teils mangele es

bei den Verantwortlichen an Vorstellungskraft, wie kreativ Cyberkriminelle sind. Und diese Fehleinschätzung bestehender Risiken hat nach Erfahrung des Experten wiederum fatale Folgen für das IT-Budget personell wie finanziell. „Wenn Sicherheitslücken bestehen, hat das nicht zwingend mit einer mangelnden Kompetenz der IT-Mitarbeiter zu tun – sondern vielmehr mit fehlendem Personal und einer zu geringen finanziellen Ausstattung."

Bei den untersuchten Unternehmen kommt im Schnitt eine IT-Kraft auf 87 Mitarbeitende. Für Mittelständler mit ZOO Beschäftigten bedeutet das, sie haben Z,Z Angestellte, die sich um die gesamten IT-Systeme des Betriebes inklusive des Maschinenparks kümmern und alles am Laufen halten müssen für Prävention und die ständige Verbesserung der IT-Sicherheit bleibt dann kaum noch Zeit. Je kleiner das Unternehmen, desto größer übrigens das Problem: Ein Drittel der untersuchten Betriebe beschäftigt gar keine eigenen IT-Kräfte – alle diese Firmen haben weniger als 100 Mitarbeiter.

## Zu oft steht Sicherheit nur auf dem Papier

Was können kleine und mittelständische Unternehmen tun, um der wachsenden Gefahr durch Cyberangriffe zu begegnen? Sie müssen IT-Sicherheit leben – und das bedeutet, IT-Sicherheit muss Managementaufgabe sein, meint White-Hat-Hacker Wiesner. Ein so genanntes Information Security Management System (ISMS) kann hier ein sinnvolles Instrument sein. Ein solches Konzept definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen zu gewährleisten. Ganz zentral dabei: Es verfolgt einen Top-Down-Ansatz ausgehend von der Unternehmensführung.

Ein ISMS nützt allerdings wenig, wenn es nur auf dem Papier steht, wie auch die aktuelle Untersuchung zeigt. Nach eigenen Angaben besitzen nämlich sechs der 40 Unternehmen Grundzüge eines ISMS, eines betreibt sogar ein vollständiges. „Ausgerechnet eines dieser Unternehmen war es, in das wir am leichtesten eindringen konnten", sagt Wiesner.

Ob mit ISMS oder ohne – schon mit eigentlich selbstverständlichen technischen Maßnahmen lässt sich eine verbesserte Sicherheit gegen Hacker erzielen. „Zum Beispiel, indem Unternehmen ihre Betriebssysteme aktuell halten, regelmäßig Sicherheitsupdates einspielen und eine Zwei-Faktor-Authentifizierung für ihre Mitarbeitenden einführen", zählt Wiesner auf. Und auch wenn die finanziellen Mittel gerade in kleineren Produktionsbetrieben endlich seien, sei IT- und Maschinensicherheit gut umsetzbar: „Ein wichtiger Faktor neben mehr Geld und mehr Personal und Konzepten wie einem Informationssicherheitsmanagementsystem ist: die Kommunikation."

Hier sind alle Mitarbeitenden gefragt. Regelmäßige Phishing-Kampagnen beispielsweise könnten Belegschaften für die Gefahren, die dort lauern, sensibilisieren. „Und: Geschäftsführung und IT-Verantwortliche müssen mehr miteinander reden." Managemententscheidungen können nur so gut sein, wie die Informationen, auf denen sie beruhen. „In zu vielen Unternehmen lebt noch das Klischee von den IT-Mitarbeitenden, die im Keller sitzen und Pizza bestellen und ansonsten die Bürotür am liebsten geschlossen halten."

*© spiegel.de, Patrick Beuth*

*Montag, 16.Oktober 2019*

***Hunderte Server ausgefallen***

# Massive IT-Störung legt Porsche-Produktion lahm

## Mehr als 200 Server von Porsche waren am Dienstag ausgefallen: Nach SPIEGEL-Informationen stand dadurch nicht nur die Produktion vorübergehend still. Ausgangspunkt war ein fehlerhafter Datenspeicher.

Der Sportwagen-Hersteller Porsche musste seine Produktion im Stammwerk in Zuffenhausen sowie in Leipzig vorübergehend einstellen. Ein massiver Serverausfall war der Grund dafür.

Am frühen Dienstagabend informierte das Porsche-Management alle Mitarbeiter weltweit per E-Mail über die IT-Störung. Demnach waren alle auf SAP-Software basierenden Prozesse betroffen. Ab Mittag seien erste Probleme gemeldet worden, in den folgenden Stunden zeigte sich das ganze Ausmaß der Störung, heißt es.

In Zuffenhausen, wo mehr als 7000 Mitarbeiter täglich rund 200 Autos vom Band lassen, kam die Fertigung durch den IT-Ausfall zunächst komplett zum Stillstand. Auch in Leipzig, wo der Panamera und der Macan gefertigt werden, kam die Produktion zum Erliegen.

Nicht nur die Herstellung, auch Ersatzteillager und Kundenprozesse fielen komplett aus. 211 Server waren von den Problemen betroffen, heißt es in der Rundmail. Eine Möglichkeit, über Ersatzserver oder andere Umwege die Produktion wieder zum Laufen zu bringen, gab es demnach zunächst nicht.

Am Dienstagabend sei die Produktion aber schrittweise wieder angelaufen, teilte ein Porsche-Sprecher dem SPIEGEL am Mittwoch mit. Ein Angriff von außen oder eine Infektion mit Schadsoftware war seinen Angaben zufolge nicht der Grund für die Störung. Ein fehlerhafter Datenspeicher war der Ausgangspunkt, präzisierte Porsche später, es habe sich also um ein Hardware-Problem gehandelt. Allerdings habe eine Software, die Auswirkungen auf weitere Systeme hätte stoppen sollen, nicht funktioniert. Der Produktionsausfall werde aber „keine nachhaltigen wirtschaftlichen Auswirkungen“ auf Porsche haben, sondern wieder aufgeholt werden.

**Pilz Gruppe: „Sämtliche Computersysteme vom Netz“**

Bereits am Sonntag sind beim Automatisierungsspezialisten Pilz aus Ostfildern „sämtliche Computersysteme vom Netz genommen“ worden. Das Unternehmen sieht sich anders als Porsche aber als „Opfer eines gezielten Cyberangriffs“. Betroffen seien „weltweit sämtliche Server- und PC-Arbeitsplätze inklusive des Kommunikationsnetzwerkes“, teilt die Pilz Gruppe mit . Die Störungen würden „noch einige Tage andauern“. Mehr wollte eine Unternehmenssprecherin auf SPIEGEL-Anfrage nicht dazu sagen, sie verwies auf die laufenden Ermittlungen des Landeskriminalamtes.

In den vergangenen Jahren hat Schadsoftware in verschiedenen deutschen Unternehmen vergleichbare Auswirkungen gehabt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte bereits im Dezember und zuletzt noch einmal im September von mehreren Fällen gesprochen, in denen es durch die Malware Emotet „große Produktionsausfälle“ gab, „da ganze Unternehmensnetzwerke neu aufgebaut werden mussten“.

Die Ransomware WannaCry wiederum befiel 2017 innerhalb weniger Tage weltweit rund 200.000 Rechner und sorgte für Schäden von mindestens mehreren Hundert Millionen Euro, andere Schät-

zungen gingen in den Milliardenbereich. Auch damals war ein Autohersteller betroffen: Renault in Frankreich.

Die Malware NotPetya hatte kurz darauf sogar für Schäden in Höhe von geschätzt zehn Milliarden Dollar gesorgt, indem sie sich rasend schnell verbreitete und Daten auf befallenen Rechnern unwiederbringlich verschlüsselte.

*Mittwoch, 16. Oktober 2019*

***Pilz-Chef: „Wir werden erpresst“***

# IT-Ausfall: Stillstand bei Porsche und Pilz

## Porsche musste wegen eines Serverausfalls die Produktion in zwei Werken stoppen. Auch Pilz leidet unter einem Ausfall der IT. Der Automatisierungsspezialist wurde Opfer eines Hackerangriffs – und erklärt im Video, was genau passiert ist.

Der Automatisierungsspezialist Pilz aus Ostfildern hat derzeit Probleme bei der IT, wie Geschäftsführer Thomas Pilz auf dem Maschinenbau-Gipfel in Berlin berichtete. Das Unternehmen wurde Opfer eines Hackerangriffs. „Wir hoffen, dass wir am Montag unsere Server wieder zum Laufen bringen können, momentan geht nix“, so Thomas Pilz gegenüber „Produktion“ auf dem Gipfeltreffen des deutschen Maschinenbaus.

Holger Paul, Leiter Kommunikation des Maschinenbauverbands VDMA, kommentierte diesen Vorfall auf Twitter: „Die bittere Ironie nach einem Cyberangriff: das BSI will dem Mittelstand nicht helfen, aber der Betriebsprüfer kommt trotzdem und will Belege sehen. Thomas Pilz schildert die Realität nach dem Hackerangriff auf seine Firma auf dem Maschinenbau-Gipfel.“

Pilz selbst machte auf dem Gipfeltreffen eine klare Ansage: Der Maschinenbauer werde kein Lösegeld an Hacker-Erpresser zahlen.

### Server-Ausfall bei Porsche – Produktion stand still

Auch Porsche leidet unter IT-Problemene. Laut dem „Spiegel“ fielen bei dem Autobauer mehr als 200 Server aus. Am frühen Dienstagabend informierte das Porsche-Management alle Mitarbeiter weltweit per E-Mail über die IT-Störung. Demnach waren alle auf SAP-Software basierenden Prozesse betroffen. Ab Mittag seien erste Probleme gemeldet worden, in den folgenden Stunden zeigte sich das ganze Ausmaß der Störung, heißt es in dem Bericht.

Massiv betroffen waren die Werke Zuffenhausen und Leipzig. In beiden kam die Produktion zum Erliegen. Darüber hinaus waren auch Ersatzteillager und Kundenprozesse des Autobauers von dem Serverausfall betroffen.  Eine Möglichkeit, über Ersatzserver oder andere Umwege die Produktion wieder zum Laufen zu bringen, gab es demnach zunächst nicht.

Gegenüber dem „Spiegel“ erklärte ein Porsche-Sprecher, dass es sich nicht um einen externen Hackerangriff gehandelt habe. Ein intern entstandenes Problem sei der Grund für den Produktionsstopp gewesen.

Am Dienstagabend sei die Produktion jedoch schrittweise wieder angelaufen. Zum entstandenen Schaden machte der Porsche-Sprecher zunächst keine Angaben, ebenso wenig zu den technischen Details der Störung.

### Wie sich Maschinenbauer über den VDMA gegen Cyberangriffe versichern können

Um genau solche Angriffe wie bei Pilz abzusichern, hat die 100prozentige VDMA-Tochter VSMA eine speziell auf die Bedürfnisse von Maschinenbauern zugeschnittene Versicherung entwickelt.

„Diese Versicherung deckt verschiedene Bereiche ab – von Kosten durch Betriebsunterbrechung, über Schäden bei Kunden bis hin zu teilweiser Erstattung von Lösegeldern“, erklärt Jürgen Seiring von VSMA. Auch eine Notfallplanung und die Einschaltung von Forensikern zur Beseitigung der Schadsoftware sind Teil der Versicherung.

*Dienstag, 2. Juli 2019*

**Hackerangriff**

# So dreist kassieren Cyber-Erpresser Lösegeld von Wempe

## Kriminelle griffen Juwelier bereits vor einer Woche an. Die Firma ist nicht das erste Opfer. Polizei geht von Milliardenschäden aus.

Hamburg. Der Hamburger Traditions-Juwelier Wempe ist Opfer einer Cyber-Erpressung geworden. „Eine Gruppe professioneller Täter blockierte unser Computersystem mit einer speziellen Software. Durch diese Erpressungssoftware (sogenannte Ransomware) waren unsere Server verschlüsselt. Das war eine Geiselnahme unserer Daten auf unseren eigenen Servern“, sagte Sprecherin Nadja Weisweiler auf Abendblatt-Anfrage.

### Wempe-Erpressung begann vor einer Woche

Der Vorfall ereignete sich bereits am Montag vor einer Woche. Auf den Servern hatten die Erpresser eine Nachricht und eine E-Mail-Adresse zur Kontaktaufnahme hinterlassen. Die Kriminellen forderten Lösegeld. Als Gegenleistung sollte der 1878 gegründete Juwelier – mit Filialen in der ganzen Welt – ein Passwort erhalten, um wieder auf die eigenen Server und damit auf die verschlüsselten Daten zugreifen zu können.

„Naturlich haben wir umgehend das Landeskriminalamt (LKA) der Hamburger Polizei informiert, das dann die Ermittlungen aufgenommen hat“, sagte Sprecherin Weisweiler. Die Server seien umgehend vom Netz genommen und externe Experten fur IT-Forensik und IT-Sicher- heit hinzügezogen worden.

Ein Sprecher der Hambürger Polizei bestätigte dem Abendblatt: „Wir führen derzeit ein Ermittlungsverfahren wegen Verdachts der Erpressung und der Datensabotage zum Nachteil eines Hamburger Unternehmens. Nach dem bisherigen Erkenntnisstand wurden dabei die auf einem Server abgelegten Daten des Unternehmens angegriffen, verschlüsselt und Forderungen zu deren Wiederherstellung gestellt.“

### Wempe musste Rechnungen per Hand schreiben

Auf den Computern sind auch Tausende Kundendaten gespeichert. Aber auf diese hatten es die Täter offensichtlich nicht abgesehen: „Nach dem derzeitigen Stand der Analyse gibt es keine Hinweise auf die Entwendung der Daten unserer Kunden und Geschäftspartner“, sagte Weisweiler.

Neben dem LKA informierte Juwelier Wempe auch den Hamburgischen Beauftragten für Datenschutz über die Cyber-Attacke. Der Geschäftsbetrieb in den weltweit 34 Niederlassungen ging trotz des Vorfalls weiter. Die Kassen waren von der Cyber-Erpressung nicht betroffen. Allerdings konnten keine Rechnungen ausgedruckt werden und wurden deshalb per Hand geschrieben. Lediglich bei der Wartung von Uhren komme es zu Verzögerungen, sagte Weisweiler.

### Abendblatt exklusiv: Wempe zahlte Lösegeld

Nach exklusiven Abendblatt-Informationen bezahlte Juwelier Wempe schließlich ein Lösegeld an die

Kriminellen und erhielt daraufhin das Passwort. Die Höhe ist nicht bekannt. Aktuell liege das Hauptaugenmerk auf der Wiederherstellung der Systeme. Dabei werde vorsichtig und mit Bedacht vorgegangen, so Weisweiler. Auch der Hamburger Beiersdorf Konzern wurde in der Vergangenheit bereits Opfer einer Cyber-Attacke.

---

Was will die Politik?
Hamburgs FDP fordert seit Langem, dass die technische Ausstattung der Polizei verbesser werden muss, damit man diese Cyberangriffe auch zurückverfolgen kann. Ende Mai hat Justizsenator Till Steffen (Grüne) eine Bundesratsinitiative mit dem Ziel einer umfassenden Reform des Computerstrafrechts eingebracht. Die bisherige Gesetzgebung im Bereich Cyber- crime sei lückenhaft, ein einziges Flickwerk. Andererseits dürfe ein modernes Computerstrafrecht auch nicht so ausgestaltet werden, dass es die Freiheiten des Einzelnen bedroht.

---

Wie die Erpresser via Internet vorgehen und wie sich Firmen schützen können, gibt eine kleine Übersicht:

### Was ist Cyberkriminalität?

Weit überwiegend handelt es sich dabei um Computerbetrug, rund 75 Prozent aller Cybercrime-Straftaten gehen darauf zurück. Dabei greift der Täter ohne Erlaubnis in die Funktion eines Computerprogramms ein, verursacht so einen Vermögensschaden und verschafft sich selbst einen Vermögensvorteil. Weiter fallen unter Cybercrime zum Beispiel unrechtmäßige Abbuchungen von Online-Konten. Auch Computersabotage, das Ausspähen von Daten oder die missbräuchliche Nutzung von Telekommunikationsdiensten sowie Datenveränderung fallen in den Deliktbereich.

### Wie gefährlich ist Cybercrime?

In kaum einen anderen Deliktbereich steigen die Fallzahlen derart rasant wie bei der Cyberkriminalität. Und doch sind die Fälle, die der Polizei gemeldet werden, nur die Spitze des Eisbergs, wie das Bundeskriminalamt (BKA) konstatiert. Die polizeiliche Kriminalstatistik gebe „nicht annähernd“ die tatsächliche Häufigkeit von übers Internet gesteuerten Attacken gegen Firmen oder private Nutzer wieder. „Es muss von einem sehr großen Dunkelfeld ausgegangen werden“, so das BKA. Häufig zahlen die Firmen dann lieber schweigend ein Lösegeld, als sich einem vermeintlichen Imageschaden auszusetzen. Die Täter wiederum verschleiern häufig ihre Identität und operieren anonym vom Ausland aus.

### Wie gehen die Täter vor?

Insbesondere mittelständische Unternehmen sind von einem massenhaften Befall ihrer Daten und Netzwerke betroffen. Am häufigsten infizieren die Täter fremde Computersysteme mit Schadsoftware, um beispielsweise an sensible Daten zu gelangen oder um von den Unternehmen ein Lösegeld zu erpressen, indem sie durch Verschlüsselung ganze Firmennetzwerke lahmlegen und so den Zugriff sperren. Zuletzt hat der Trojaner „Emotet“ der Hamburger Polizei viel Sorge bereitet. Die Schadsoftware verwendet zur Tarnung täuschend echt aussehende Mails angeblicher Freunde oder Geschäftspartner. Es gibt aber auch die Variante mit verseuchten Bewerbungsmails. Wird die angefügte Datei geöffnet, verbreitet sich die Schadsoftware mitunter im gesamten Netzwerk.

### Gibt es Fälle in Hamburg?

Sehr viele. Nur die wenigsten werden aber bekannt, wie der Hackerangriff auf den Konzern Beiersdorf im Juni 2017. Vermutlich gelang es den Tätern, die Buchhaltungssoftware einer Firmenfiliale in der Ukraine während eines Updates zu manipulieren. Folge: Der Trojaner verschlüsselte wichtige Da-

teien und machte die Computer im Netzwerk praktisch unbenutzbar. Von einem ähnlichen Schädling wurde auch die dänische Maersk-Gruppe im Juni 2017 heimgesucht – die gesamte digitale Infrastruktur des Reederei-Riesen brach zusammen. Die Täter verlangen dann meist ein Lösegeld zur Entschlüsselung der Dateien, zahlbar in der Krypto-Währung Bitcoin.

### Wie hoch ist der Schaden?

Der Schaden durch Cybercrime kann auch aufgrund des zurückhaltenden Anzeigeverhaltens der Geschädigten nur geschätzt werden. Nach einer anonymen Befragung des Digitalverbandes Bitkom sind mittelständische Unternehmen am häufigsten von Attacken betroffen, aber auch Großfirmen und Handwerksbetriebe sind nicht davor gefeit. Laut Bitkom hat in den Jahren 2017 und 2018 ein Viertel aller deutschen Industrieunternehmen einen Angriff durch Schadsoftware registriert. Der Schaden geht in Deutschland in die Milliarden Euro, weltweit, so die Polizei, wird der Schaden durch Cyberkriminelle auf mehr als 350 Milliarden Euro geschätzt.

### Operieren die Täter nur am Computer?

Nicht unbedingt. Wie akut existenzgefährdend sich digitale kriminelle Machenschaften im echten, analogen Leben auswirken können, hat eine mittelständische Hamburger Firma vor gut einem Jahr erfahren müssen: Ein Angestellter der IT, zuständig für das Computer-Netzwerk, wechselte damals zu einem Konkurrenten und brachte seinem neuen Arbeitgeber ein „Willkommensgeschenk“ mit: kurz vor seinem Abgang hatte sich der Mitarbeiter noch umfassenden Zugriff auf das Netzwerk seines alten Arbeitgebers verschafft. So gelang es dem neuen Arbeitgeber, die Kommunikation des Konkurrenten auszuspähen und ihn bei Ausschreibungen regelmäßig zu unterbieten. Bevor der Betrug aufflog, stand das bespitzelte Unternehmen mit dem Rücken zur Wand.

### Wie kann man sich schützen?

Die Polizei rät dazu, bei der Sicherung der IT-Infrastruktur nicht zu sparen. Besser dran sind Unternehmen grundsätzlich, wenn sie auf ein „gutes und professionell gewartetes Backup- System setzen“, um im Ernstfall ihre Daten aus nicht infizierten Quellen wiederherstellen zu können, sagt Andreas Dondera, Leiter der Zentralen Ansprechstelle Cybercrime (ZAC) bei der Hamburger Polizei. Auch eine Schulung der Mitarbeiter ist entscheidend, denn in den meisten Fällen gelangt Schadsoftware überhaupt nur durch einen menschlichen Fehler ins Netzwerk. Die Polizei setzt auf Prävention, stellt für Unternehmen im Internet Tipps zur Cyber- Sicherheit zur Verfügung.

*Dienstag, 8. Januar 2019*

**Massenhafter Datenklau**

# „Ärger" über Politik trieb Hacker

## Der 20-jährige Verdächtige im Fall des Datenklaus bei Politikern und Prominenten ist geständig. Laut Ermittlern gibt er an, allein gehandelt zu haben. Sein Motiv: „Ärger" über die aktuelle Politik.

Der nach dem massiven Online-Angriff auf Politiker und Prominente vorübergehend festgenommene 20-jährige Deutsche hat in einer Vernehmung Ärger über Äußerungen seiner Opfer als Motiv für seine Taten genannt. Das teilte Oberstaatsanwalt Georg Ungefuk, Sprecher der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) der Generalstaatsanwaltschaft Frankfurt am Main, mit.

Ermittler hatten den jungen Mann, der noch bei seinen Eltern wohnt, am Wochenende in Mittelhessen festgenommen. Laut Ungefuk handelt es sich bei dem Beschuldigten um einen „sehr computeraffinen" Menschen, der aber über keine entsprechende Ausbildung verfüge und nicht vorbestraft sei. Der Mann habe viel Zeit damit verbracht, sich am PC bestimmte Kenntnisse anzueignen. Bei der Vernehmung habe er die Tat eingeräumt und umfassend mit den Ermittlern kooperiert. Zudem habe er erklärt, dass er allein gehandelt habe. Die bisherigen Ermittlungen hätten keine Hinweise auf eine Beteiligung weiterer mutmaßlicher Täter gegeben.

### Beschuldigter zeigt Reue

Der Mann wurde nach der Vernehmung auf freien Fuß gesetzt. Es gibt „eine klare Reue-Reaktion", sagte Ungefuk. Der 20-Jährige sei bei der Ausspähung und Veröffentlichung der privaten Daten möglicherweise unbedacht oder leichtfertig gewesen. Bei jüngeren Tätern erlebe man oft, dass dann, wenn plötzlich die Polizei vor der Tür stehe, doch „ein großes Nachdenken einsetzt", so Ungefuk. Derzeit werden die beschlagnahmten Datenträger untersucht. Offenbar gelang es dem 20-Jährigen noch vor der Durchsuchung der Wohnung einen Speicherträger zu vernichten. Reste des gelöschten Datenmaterials konnten aber gesichert werden.

Bei seinem Datenklau hat der 20-Jährige mehrere Sicherheitslücken ausgenutzt. Für die Tat sei ein „gewisser technischer Sachverstand" nötig gewesen, sagte Ungefuk. Dem jungen Mann sei es durch eine „ausgeklügelte Vorgehensweise" gelungen, die Daten auszuspähen. Es habe nicht nur eine, sondern mehrere Ausspähaktionen gegeben, vor allem im Jahr 2018. Zudem habe er Daten aus öffentlich zugänglichen Quellen zusammengetragen. Einige Sicherheitslücken seien inzwischen geschlossen worden.

Der 20-Jährige soll über das inzwischen gesperrte Twitter-Konto @_0rbit im Dezember zahlreiche persönliche Daten von Politikern und Prominenten als eine Art Adventskalender veröffentlicht haben. Rund 1000 Politiker, Prominente und Journalisten sind nach Angaben des Bundesinnenministeriums von dem Online-Angriff betroffen. Etwa 50 Fälle seien schwerwiegender, weil größere Datenpakete wie Privatdaten, Fotos und Korrespondenz veröffentlicht wurden.

*Donnerstag, 17. Januar 2019*

# Millionen gestohlener Passwörter im Netz aufgetaucht

## Im Internet ist ein unverschlüsselter Datensatz mit gestohlen Log-in-Informationen aufgetaucht.

Im Internet stößt ein australischer IT-Experte auf einen riesigen Datensatz mit gestohlenen E-Mail-Adressen und Passwörtern. Millionen Menschen weltweit sind von dem Datendiebstahl betroffen. Über einen kostenlosen Dienst können Nutzer überprüfen, ob sie betroffen sind.

Im Internet ist ein gewaltiger Datensatz mit gestohlenen Log-in-Informationen aufgetaucht. Darin enthalten seien knapp 773 Millionen verschiedene E-Mail-Adressen und über 21 Millionen im Klartext lesbare unterschiedliche Passwörter, berichtete der australische IT-Sicherheitsexperte Troy Hunt. Insgesamt umfasse die Sammlung mit dem Namen „Collection #1" mehr als eine Milliarde Kombinationen aus beiden.

Der 87 Gigabyte große Datensatz bündele Informationen „aus vielen einzelnen Datendiebstählen und Tausenden verschiedenen Quellen", schrieb Hunt in einem Blogeintrag. Der in der Szene sehr geschätzte Security-Experte erklärte weiter, es handle sich um den größten einzelnen Datensatz dieser Art, mit dem er bislang zu tun gehabt habe. Betroffen sind Internetnutzer weltweit – darunter auch Anwender aus Deutschland.

Wer überprüfen will, ob seine E-Mail-Adresse in der Sammlung auftaucht, kann Hunts Dienst haveibeenpwned.com nutzen. In der Datenbank wird die Adresse mit Abermillionen Informationen aus Datenlecks abgeglichen. Er habe auch die jüngsten Daten dort eingepflegt, erklärte der Microsoft-Mitarbeiter Hunt. Spätestens wenn die eigene Mail dort auftauche, solle man über ein neues Passwort und wenn möglich über eine Zwei-Faktor-Authentifizierung nachdenken, sagte Linus Neumann vom Chaos Computer Club.

### Experte rät zu zufälligen Passwörtern mit maximaler Länge

„Das Jahr ist gerade mal zwei Wochen alt und es ist bereits das zweite Mal, dass wir alarmierende Nachrichten haben", sagte er auch mit Blick auf den massiven Online-Angriff auf knapp 1000 Politiker und Prominente, der Anfang Januar publik geworden war. „Es gibt keine Ausreden mehr. Jeder der nichts für seine Sicherheit macht, handelt fahrlässig und geht ein Risiko ein."

Neumann rät, bei allen Diensten ein jeweils anderes und zufälliges Passwort mit maximaler Länge zu nutzen. Dieses solle dann über einen Passwort-Manager verwaltet werden. Bei der von Neumann empfohlenen Zwei-Faktor-Authentifizierung entriegeln Nutzer den Zugang zu ihrem Onlinekonto oder Social-Media-Profil zusätzlich zum Passwort durch eine weitere Abfrage auf einem anderen Weg. Das kann beispielsweise eine SMS oder eine Code-Abfrage sein.

Laut Hunt können die Datensätze besonders für das sogenannte „Credential Stuffing" missbraucht werden. Bei dieser Methode nutzen die Angreifer die Kombination aus E-Mail und Passwort, um sich auch bei anderen Diensten – beispielsweise bei Soziale Netzwerken oder Shopping-Plattformen einzuloggen. Die Hacker gleichen dabei lange Listen mit Log-in-Daten automatisch mit den Zugangssystemen ab.

In den vergangenen Jahren hatte es diverse Hacker-Attacken gegeben, bei denen zum Teil Hunderte Millionen Kombinationen aus E-Mail-Adressen und Passwörtern erbeutet worden waren. Die Passwörter waren dabei aber größtenteils kryptografisch verschlüsselt gewesen.

*Donnerstag, 11. Oktober 2018*

***Mehr Schadprogramme im Umlauf***

# Cyber-Kriminelle setzen auf neue Methoden

**Kriminelle im Internet werden immer raffinierter. Sie könnten sich sogar in Herzschrittmacher einklinken und diese umprogrammieren, heißt es in einem neuen Behörden-Bericht. Um an Geld zu kommen, schwenken die Hacker demnach auf eine neue Methode um.**

Cyber-Kriminelle schwenken von Erpresser-Software zunehmend auf lukrativere Aktivitäten um. Angriffe mit sogenannter Ransomware scheinen in dem Maße abzunehmen, wie andere Geschäftsmodelle wie etwa das illegale Krypto-Mining zunehmen, schreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem jährlichen Lagebericht. Das BSI ist zuständig für die Abwehr von Cyberangriffen und berät Verbände und Unternehmen.

Bei der illegalen Variante des Krypto-Minings kapern Kriminelle mit Hilfe von Schadsoftware die Rechner, um die Kapazität für das „Schürfen" digitaler Währungen wie Bitcoin zu nutzen. Die Opfer bleiben zum Teil auf hohen Strom-Rechnungen für den erheblichen Energiebedarf sitzen. Bei Ransomware-Angriffen sperren die Angreifer hingegen bestimmte Dateien oder gar ganze Rechner und verlangen von den Betroffenen Lösegeld für die Freischaltung.

Das passierte etwa im Mai 2017 bei der weltweiten WannaCry-Attacke, bei der mehr als 300.000 Computer in 150 Ländern infiziert wurden, darunter auch bei der Deutschen Bahn und in britischen Krankenhäusern. Bei den Schadprogrammen im Umlauf registrierte das BSI eine kräftige Zunahme: Die Zahl stieg von mehr als 600 Millionen im Jahr 2017 auf mehr als 800 Millionen 2018. Die Zahl der Schadprogramm-Varianten pro Tag sei von 280.000 auf 390.000 gestiegen. Der Bericht deckt den Zeitraum vom 1. Juli 2017 bis zum 31. Mai 2018 ab.

Neue Angriffsziele entstehen mit der zunehmenden Vernetzung von Alltagsgegenständen wie Stromzählern, Heizungen oder auch Medizinprodukten. So sei es unter Laborbedingungen etwa gelungen, Herzschrittmacher oder Beatmungsgeräte zu hacken und umzuprogrammieren, schreibt das BSI in seinem Bericht. Gleichzeitig werde gerade bei solchen Geräten auf eine bessere Verschlüsselung verzichtet, etwa um Ärzten im Notfall einen raschen Zugriff zu ermöglichen. Da die Gefährdungslage kritisch sei, müsse noch stärker an speziellen Sicherheitsmechanismen geforscht werden.

## Grüne fordern IT-Sicherheitsgesetz

Die Grünen werfen der Bundesregierung derweil Nachlässigkeit bei der IT-Sicherheitspolitik vor. „Derzeit erreichen uns täglich Meldungen über verheerende Datenskandale und geheimdienstliche Versuche, digitale Infrastrukturen und private Kommunikation zu kompromittieren", sagte der Vize-Fraktionschef der Grünen, Konstantin von Notz. „Die Einschläge kommen täglich näher und die Gefahr eines neuen Kriegsschauplatzes im Digitalen ist durchaus real."

*Freitag, 28. September 2018*

***50 Millionen Profile betroffen***

# Facebook meldet Hackerattacke

**Facebook erlaubt Nutzern, ihr eigenes Profil zu betrachten. Über diese Funktion aber schlichen Angreifer ins soziale Netzwerk. Inzwischen ist die Lücke wieder verschlossen, das genaue Ausmaß des Angriffs aber noch unklar.**

Ein halbes Jahr nach dem Facebook-Datenskandal um Cambridge Analytica stellt nun ein massiver Hacker-Angriff das Vertrauen der Nutzer auf die Probe. Fast 50 Millionen Mitglieder des weltgrößten Online-Netzwerks sind direkt betroffen. Die Angreifer hätten digitale Schlüssel zu ihren Accounts gestohlen, mit denen sie „die Profile nutzen konnten als seien es ihre eigenen", sagte Facebook-Manager Guy Rosen.

Nach bisherigen Erkenntnissen hätten die Hacker aber keine privaten Nachrichten abgerufen oder versucht, etwas im Namen der betroffenen Nutzer bei Facebook zu posten, hieß es. Zugleich hätten die Angreifer aber in großem Stil Profil-Informationen wie Name, Geschlecht und Wohnort abgerufen. Dadurch sei die Attacke auch aufgefallen. Bisher habe Facebook keinen Fokus auf bestimmte Regionen oder Nutzergruppen feststellen können.

Erschwerend kommt hinzu, dass die Angreifer sich mit den erbeuteten Digitalschlüsseln auch bei anderen Online-Diensten anmelden konnten, die mit dem Facebook-Login genutzt wurden. Ob es dazu kam, ist bisher unklar. Die Sicherheitslücke sei am Donnerstag geschlossen worden, betonte Facebook.

### Auch Zuckerbergs Profil betroffen

Zumindest gemessen an der Zahl betroffener Nutzer ist es der bisher größte Hacker-Angriff auf das Online-Netzwerk. „Wir wissen nicht, wer hinter dieser Attacke steckt", sagte Facebooks Gründer und Chef Mark Zuckerberg in einer eilig einberufenen Telefonkonferenz. Man werde das möglicherweise auch nie erfahren, führte Produktchef Rosen hinzu. Auch die Profile von Zuckerberg und Geschäftsfuhrerin Sheryl Sandberg seien betroffen gewesen, berichteten die „New York Times" und die „Financial Times".

Die Angreifer hätten eine Sicherheitslücke in der Funktion ausgenutzt, mit der Facebook-Mitglieder sich ihr Profil aus der Sicht anderer Nutzer anzeigen lassen können, erläuterte das Unternehmen. Die Schwachstelle erlaubte es ihnen demnach, die sogenannten Token zu stehlen – eine Art Langzeitschlüssel, der auf einem Gerät gespeichert wird. Damit kann ein Nutzer schnell in sein Profil reinkommen, ohne jedes Mal ein Passwort eingeben zu müssen. Facebook stellte nach eigenen Angaben fest, dass rund 50 Millionen dieser Token gestohlen wurden. Das Passwort selbst ist dabei nicht betroffen.

Die Funktion mit der Anzeige des Profils aus Sicht von Dritten – mit der Nutzer eigentlich ihre Privatsphäre besser im Griff haben sollten – sei vorerst sicherheitshalber abgeschaltet worden, teilte Facebook weiter mit. Zur Sicherheit werden sich weitere rund 40 Millionen Nutzer auf ihren Geräten neu anmelden mussen, nur weil sie diese Funktion im vergangenen Jahr benutzt haben.

### Behörden in Irland eingeschaltet

Facebook machte keine Angaben dazu, wann genau die Hacker die Token gestohlen und damit Zu-

griff auf die Nutzer-Profile gehabt haben könnten. Facebook habe zunächst ungewöhnlich hohe Aktivität bei einer Schnittstelle am 16. September entdeckt. Am Dienstagabend dieser Woche sei man dann sicher gewesen, dass eine Attacke laufe und habe die Sicherheitslücke bis Donnerstag gefunden und geschlossen. Neben dem FBI seien gemäß der EU-Datenschutzverordnung (DSGVO) auch Behörden in Irland eingeschaltet worden.

Facebook hat insgesamt mehr als zwei Milliarden aktive Mitglieder. Die Attacke kommt zu einem extrem ungünstigen Zeitpunkt für das Online-Netzwerk, das noch um das Vertrauen der Nutzer nach dem Datenskandal um Cambridge Analytica kämpfen muss. Die Datenanalyse-Firma hatte unberechtigterweise Zugang zu Informationen von Dutzenden Millionen Nutzern bekommen. Die Enthüllung dieses Vorgangs hatte Facebook in die bisher schwerste Krise gestürzt.

Zudem versucht Facebook gerade mit größten Anstrengungen, die Plattform vor den wichtigen Kongress-Wahlen in den USA im November gegen Manipulation von außen abzusichern. Die Facebook-Aktie fiel zum US-Handelsschluss um rund 2,6 Prozent.