Bayerisches Staatsministerium des Innern und für Integration

Bayern im Netz – aber sicher!

Initiative Cybersicherheit Bayern

www.innenministerium.bayern.de

Inhaltsverzeichnis

Joachim Herrmann, MdL
Staatsminister

Gerhard Eck, MdL
Staatssekretär

Vorwort

Die Digitalisierung ist der große Megatrend unserer Zeit und verändert unsere Welt massiv – und das in immer schnelleren Schritten. Sie durchdringt inzwischen fast alle Lebensbereiche und ist ein wesentlicher Faktor für die künftige Entwicklung unserer Gesellschaft mit einer weltweiten Dimension. Die globale Vernetzung – Experten gehen von rund 50 Milliarden vernetzten Geräten im Jahr 2020 aus – bietet große Chancen für Wirtschaft und Gesellschaft und ihre Möglichkeiten erscheinen schier unerschöpflich.

Neben den vielen faszinierenden Chancen birgt diese „smarte" Welt aber auch zahlreiche Risiken. Denn durch die globale Vernetzung und Verschmelzung der Infrastrukturen mit dem Internet steigt auch die „Anfälligkeit" dieser Systeme für Cyberangriffe. Das Internet ermöglicht es Angreifern aus der Ferne auf die IT-Systeme anderer zuzugreifen und diese zu schädigen. Dabei werden die zahlreichen Schwachstellen neuer Technologien oder unzureichend geschützte Systeme skrupellos ausgenutzt.

Die Gewährleistung von Cybersicherheit ist heute ein zentrales Querschnittsthema der Inneren Sicherheit, das alle Gesellschaftsbereiche angeht. Es muss deshalb eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft sein, für ein hohes Maß

an Cybersicherheit zu sorgen. Auch wenn die primäre Verantwortung für die Sicherheit der eigenen Daten und IT-Systeme beim jeweiligen Nutzer liegt, kommt dem Staat eine Schutzfunktion zu.

Um dieser Verantwortung im Freistaat gerecht zu werden, haben wir 2013 die Bayerische Cybersicherheitsstrategie auf den Weg gebracht. Sie soll die Handlungsfähigkeit des Staates sicherstellen und für Bayerns Bürger auch im virtuellen Raum ein hohes Sicherheitsniveau gewährleisten. Ziel ist außerdem die Stärkung der Sicherheitsbehörden und eine enge Kooperation mit Wirtschaft und Wissenschaft.

Mit dieser Broschüre wollen wir für das Thema Cyberkriminalität und -sicherheit sensibilisieren, aktuelle Maßnahmen des Bayerischen Staatsministeriums des Innern und für Integration darstellen und die richtigen Ansprechpartner für staatliche Hilfen nennen.

Joachim Herrmann, MdL
Staatsminister

Gerhard Eck, MdL
Staatssekretär

1.

Chancen und Risiken der Digitalisierung

1. Chancen und Risiken der Digitalisierung

Die digitale Vernetzung ist ein zentraler Wettbewerbsfaktor für die deutsche Wirtschaft. Neben enormen Chancen entstehen damit aber auch neue Risiken.

Die Digitalisierung hat unsere Welt massiv verändert. Sie durchdringt nahezu alle Lebensbereiche – Wirtschaft, Gesellschaft und Politik – und beeinflusst alle Kommunikations- und Interaktionsformen. Die Vernetzung schreitet kontinuierlich und in immer schnelleren Schritten voran und bietet große Chancen und Möglichkeiten für die künftige Entwicklung von Wirtschaft und Gesellschaft. Ihr Potential scheint unerschöpflich: Cloud-Computing, Mobile Computing, Big Data, Industrie 4.0 und Smart Home sind Schlagwörter dieser Entwicklung.

Digitalisierung bedeutet vor allem aber auch eine zunehmende Vernetzung von Geräten und Systemen. Wie weit die Vernetzung künftig reichen wird, zeigt ein Blick auf die Fabrik der Zukunft: Maschinen, Sensoren und Steuerungsgeräte in den Produktionsanlagen sollen mit Vertrieb und Einkauf und sogar entlang der Wertschöpfungskette mit den IT-Systemen von Lieferanten, Kunden und Servicebetrieben vernetzt werden. Und auch im Privatleben verschwindet zunehmend die Grenze zwischen der realen und der virtuellen Welt: In unseren Smartphones sind Bezahl- und Gesundheitsfunktionen sowie Elemente zur Heimautomation integriert.

Das Internet ist zur entscheidenden Infrastruktur geworden und hat sich zu einem integralen Bestandteil unserer Arbeits- und Lebenswelt entwickelt. Der Gebrauch des Internets ist weltweit aus dem Alltag nicht mehr wegzudenken, er ist unverzichtbar geworden.

So faszinierend die Möglichkeiten der digitalen Revolution sind, so groß sind auf der anderen Seite die damit verbundenen Risiken und Bedrohungen für die moderne Informationsgesellschaft. Die Innovationen in der Informationstechnologie und die Komplexität der IT-Systeme eröffnen immer neue Verwundbarkeiten für Cyberangriffe und die Angreifer nutzen die Schwachstellen neuer Technologien schamlos aus. Ungeschützte Computer und Informationssysteme sind eine leichte Beute für Cyberkriminelle.

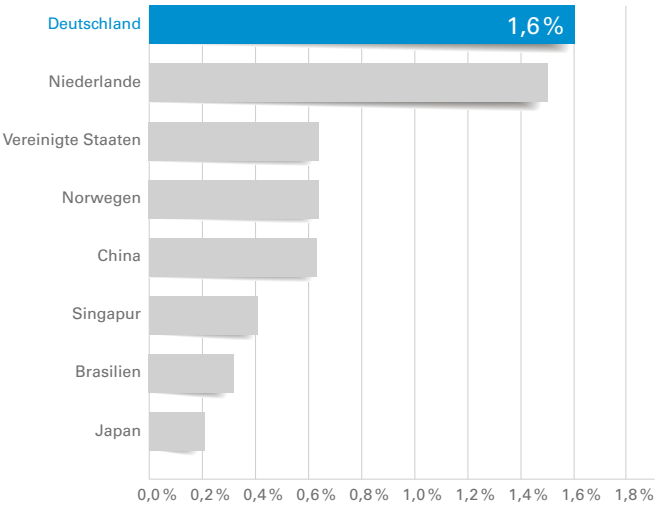
Im Fadenkreuz der Angreifer stehen Bürgerinnen und Bürger, staatliche Stellen, Wirtschaftsunternehmen, Betreiber Kritischer Infrastrukturen und wissenschaftliche Einrichtungen. Cyberangriffe können aus der Ferne von jedem Ort der Welt, zu jeder Tages- und Nachtzeit, begangen werden und sind damit für die Täter mit wenig Risiko verbunden. Die Ziele der Angreifer sind vielfältig: Mit ihnen soll längst nicht nur Geld erschlichen werden. Das Ausspähen von Daten, der Rohstoff des 21. Jahrhunderts, gehört ebenso zum Repertoire wie

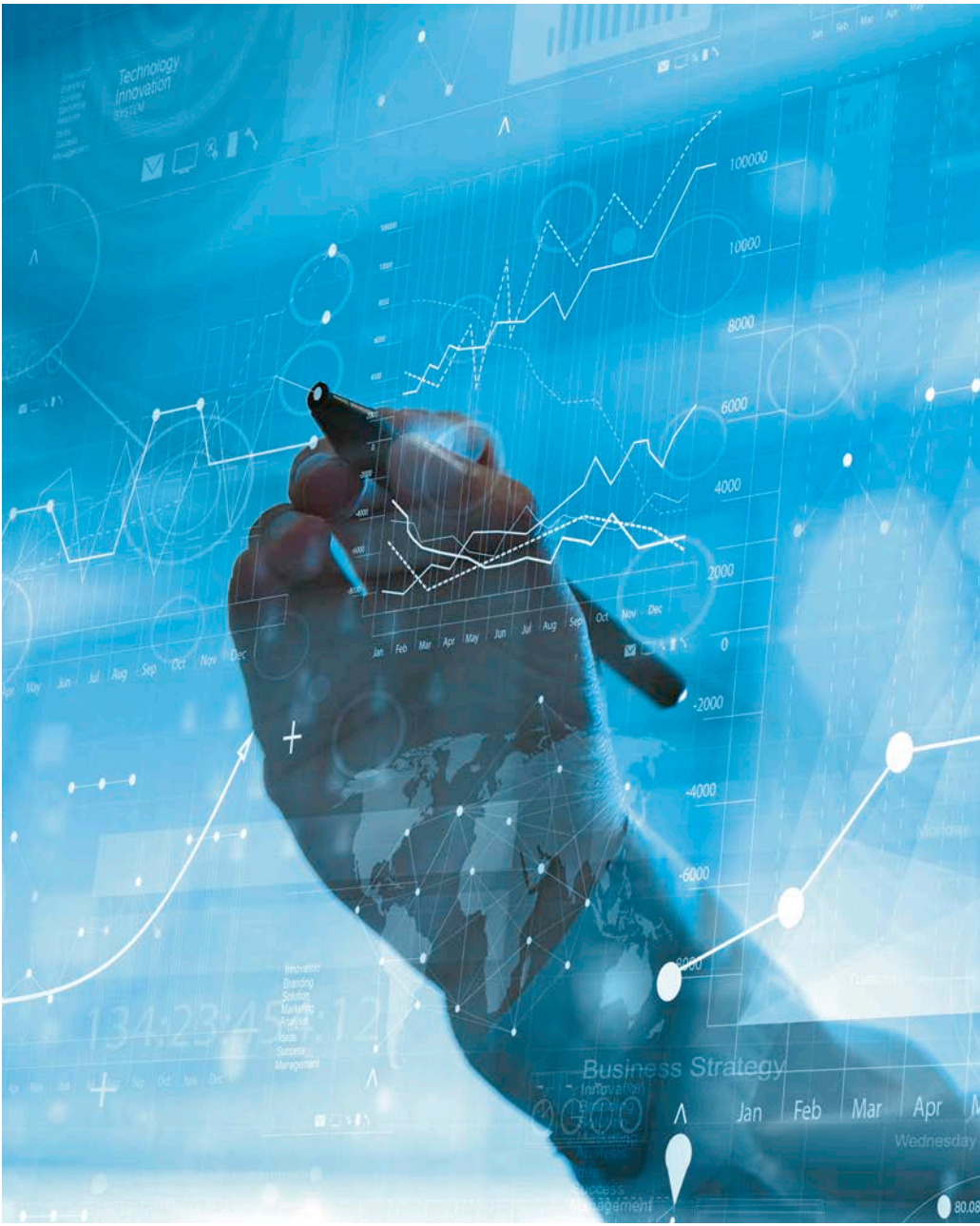
Cybersicherheit – eine große Herausforderung für Staat, Wirtschaft und Gesellschaft.

gezielte Sabotageangriffe auf Unternehmen und Betreiber Kritischer Infrastrukturen. Es geht deshalb vor allem auch darum, die „Kronjuwelen“ unserer heimischen Wirtschaft, die Basis für den Wohlstand in unserem Land, zu schützen.

Das Schadensausmaß und -potential von Cyberkriminalität ist enorm. Nach einer im Juni 2014 veröffentlichten Studie des unabhängigen Center for Strategic and International Studies in Washington kostet die Cyberkriminalität die globale Wirtschaft jährlich mehr als 400 Milliarden US-Dollar. Allein in Deutschland beträgt der wirtschaftliche Schaden im Jahr ca. 44 Milliarden Euro, das entspricht etwa 1,6% des Bruttoinlandsprodukts. Deutschland ist der Studie zufolge das von Angriffen wirtschaftlich am stärksten betroffene Land weltweit.

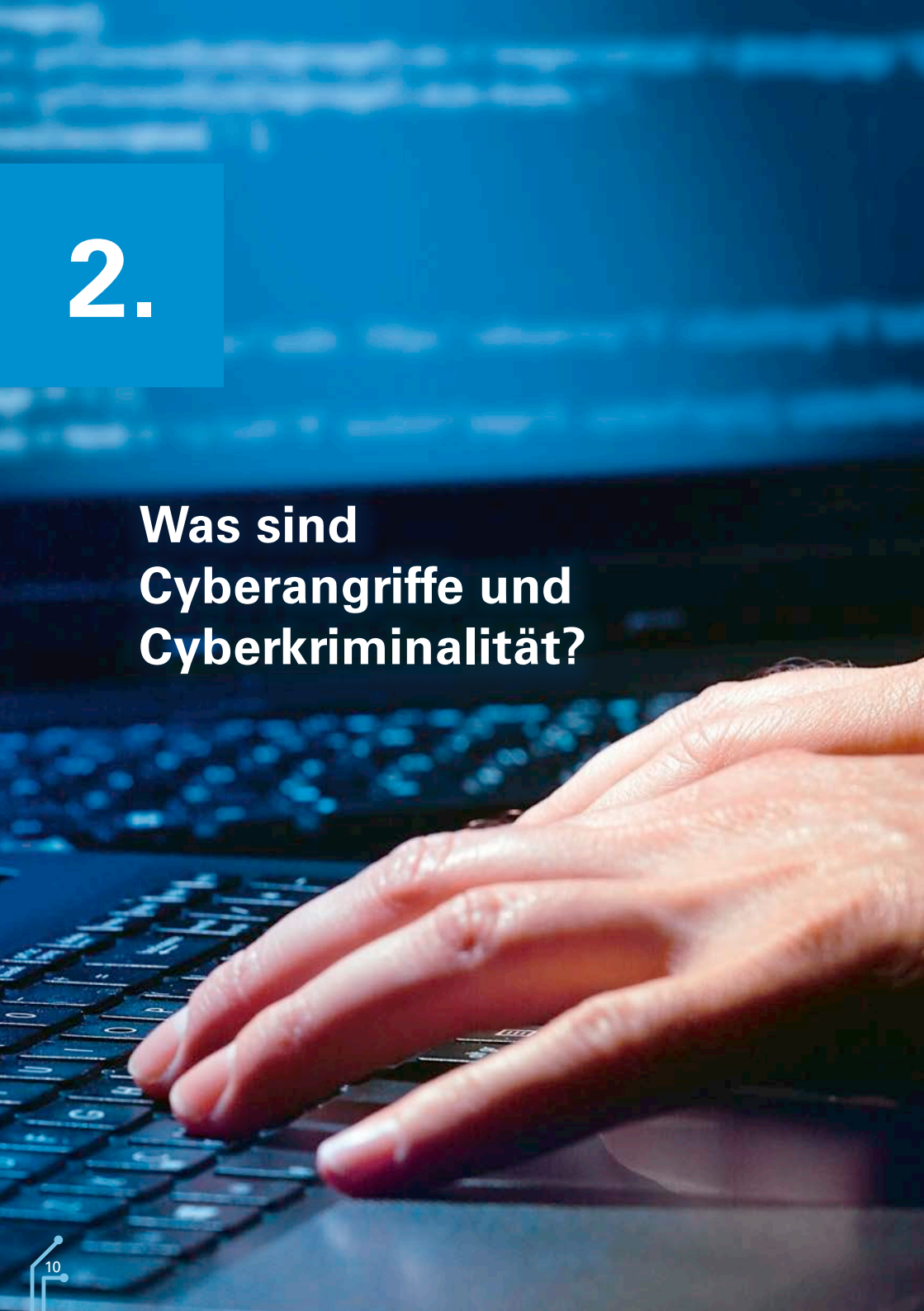
Geschätzter wirtschaftlicher Schaden durch Internetkriminalität in Prozent des nationalen Bruttoinlandsproduktes in ausgewählten Ländern im Jahr 2014




Technology
Innovation
Business Strategy
Jan
Feb
Mar
Apr
Wednesday

2.

Was sind Cyberangriffe und Cyberkriminalität?



2. Was sind Cyberangriffe und Cyberkriminalität?

Ein Cyberangriff ist ein elektronischer Angriff, der ausschließlich im virtuellen Cyberraum stattfindet und sich gegen einzelne Computer oder ganze IT-Systeme richtet. Der Angreifer will die Sicherheitsbarrieren der Systeme durchbrechen, um beispielsweise Daten auszuspähen.

Cyberkriminalität umfasst alle kriminellen Handlungen, die im Zusammenhang mit Informationstechnik und/oder dem Internet stehen. Hierzu zählen zunächst Straftaten, die sich gegen das Internet, gegen Datennetze, informationstechnische Systeme oder deren Daten richten (sogenannten Cyberkriminalität im engeren Sinn). Beispiele für solche Straftaten sind das Verbreiten von Schadsoftware (z. B. Viren, Trojaner, Würmer), Hacking (d. h. Eindringen in Informationssysteme), DDoS-Attacken oder der Aufbau und Betrieb von Botnetzen. Die Funktionsweise derartiger Angriffe wird im folgenden Kapitel näher beschrieben.

Zum anderen erfasst Cyberkriminalität aber auch „klassische" Straftaten, bei denen das Internet nur als Tatmittel dient. Ein Beispiel sind Betrugsdelikte bei Online-Geschäften, z. B. wenn via Internet bestellte Waren trotz Bezahlung nicht geliefert werden. Auch Erpressungsdelikte können mit Hilfe des Internets begangen werden. So verschaffen sich Täter beispielsweise mit einer in einer E-Mail versteckten Schadsoftware den Zugriff auf den PC oder das Smartphone, sperren das System und schalten es erst nach Zahlung eines Geldbetrages wieder frei. Oft genügt es auch schon, die Opfer allein durch Androhung einer solchen Handlung zur Zahlung zu nötigen. Die Verbreitung von Kinderpornographie findet mittlerweile schwerpunktmäßig über das Internet statt. Und auch Cybermobbing, bei dem die Opfer in Social-Media-Diensten beleidigt, bedroht und tyrannisiert werden, ist ein verbreitetes Phänomen.

Von Cyberspionage und -sabotage spricht man bei gezielten elektronischen Angriffen mit und gegen IT-Infrastrukturen. Zielen diese auf die Informationsbeschaffung, handelt es sich um Fälle von Cyberspionage. Sollen sie die IT-Systeme schädigen, spricht man von Cybersabotage. Opfer von Cyberspionage und -sabotage sind hauptsächlich Wirtschaftsunternehmen, staatliche Stellen und wissenschaftliche Einrichtungen. Angreifer können ausländische Nachrichtendienste, Konkurrenzunternehmen oder Terroristen sein.

Die Cyber-Gefährdungslage ist angespannt: Cyberangriffe sind effektiv, vergleichsweise kostengünstig und bergen ein geringes Entdeckungsrisiko.

3.

Wie gehen die Angreifer vor?

3. Wie gehen die Angreifer vor?

Schadprogramme sind eine der größten Bedrohungen im Netz. Häufig hilft der Nutzer unbewusst dabei mit, dass sein Rechner infiziert wird.

Cyberangriffe erfolgen auf vielfältige Art und Weise. Sie werden – je nach Motivation der Täter – vielseitig eingesetzt, entwickeln sich ständig fort und werden von den Opfern häufig gar nicht erkannt. Die Wirkungsweise von Angriffen ist unterschiedlich: Einerseits gibt es breit gestreute Angriffe, die eher auffallen und zeitnahe Gegenmaßnahmen erlauben. Andererseits nehmen ausgeklügelte Angriffe auf wenige gezielt ausgewählte Angriffsopfer immer mehr zu. Derartige Angriffe erfolgen regelmäßig in mehreren Angriffsschritten.

Verbreitete Angriffsmethoden sind derzeit:

› Schadprogramme

Mit Schadprogrammen (z. B. Viren, Trojaner, Würmer, Rootkits und Bots) können Angreifer die Kontrolle über infizierte PCs, Notebooks, Smartphones bis hin zu industriellen Steuerungsanlagen erlangen. Die häufigsten Verbreitungswege von Schadprogrammen sind

- Spam-Mails, die im Anhang ein Schadprogramm enthalten oder über Links zu infizierten Webseiten führen,
- Drive-By-Infektionen, d. h. die Angreifer erstellen Webseiten mit einer Schadfunktion oder manipulieren bestehende Internetpräsenzen. Die Opfer werden gezielt mit einer E-Mail kontaktiert und dazu verleitet, die infizierte Webseite über einen Link anzuklicken.

› Botnetze

Botnetze bestehen aus einer Vielzahl von Rechnern, die von einem fernsteuerbaren Schadprogramm (einem sog. Bot) befallen sind. Die betroffenen Systeme können vom Botnetzbetreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert werden, ohne dass deren Besitzer etwas davon mitbekommen. Die geballte Rechenleistung nutzen Kriminelle für den Spam-Versand, das Verbreiten von Schadsoftware, gezielte Angriffe auf Firmenrechner oder zur Verschleierung der eigenen Identität (IP-Adresse).

Von Juli 2016 bis Juni 2017 wurden täglich bis zu 27.000 Botinfektionen deutscher Systeme registriert.

› Phishing

Über gefälschte E-Mails, Webseiten oder Kurznachrichten werden die Opfer zur Preisgabe persönlicher Daten wie Konto- oder Kreditkartennummer, PINs, TANs und Kennwörter verleitet.

› Denial of Service (DoS)/Distributed Denial of Service (DDoS)

Unter einer DoS-Attacke versteht man einen Angriff auf Webserver und ganze Netzwerke mit dem Ziel, diese außer Betrieb zu setzen. Ein Server wird dabei mit so vielen Anfragen bombardiert, dass das System seine Aufgaben nicht mehr erfüllen kann und zusammenbricht. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, z. B. über ein Botnetz, spricht man von einem verteilten DoS- oder DDoS-Angriff (Distributed Denial of Service).

› Advanced Persistent Threat (APT)

Advanced Persistent Threat (APT), übersetzt „fortgeschrittene, andauernde Bedrohung", bezeichnet einen zielgerichteten Angriff auf die IT-Systeme genau ausgewählter privatwirtschaftlicher oder öffentlicher Unternehmen, Einrichtungen oder Institutionen. APT-Angriffe können nur sehr schwer verhindert werden, weil sie mit hohem Aufwand entworfen werden und die üblichen Standard-Schutzmechanismen umgehen. Nach dem erfolgreichen Angriff auf einen Rechner dringen die professionellen Täter immer weiter in die lokale IT-Infrastruktur des Opfers vor. Ziel eines APT-Angriffs ist es, möglichst lange unentdeckt zu bleiben, um über einen längeren Zeitraum sensible Informationen auszuspähen (Spionage) oder Schaden anzurichten (Sabotage).

› Social Engineering

Social Engineering (übersetzt „soziale Manipulation“) bezeichnet eine Vorgehensweise, bei der die „Schwachstelle“ Mensch ausgenutzt wird. Die Angreifer spionieren z. B. über soziale Medien oder Telefonanrufe das persönliche bzw. betriebliche Umfeld des Opfers aus, täuschen falsche Identitäten vor und versuchen, die Opfer durch Manipulation zu verleiten, Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbst Schadcodes auf ihrem PC zu installieren.

4.

Wie ist die Gefährdungslage?

4. Wie ist die Gefährdungslage?

„Bisher ist ja auch nichts passiert.“ Sind sie sicher?

4.1 Cyberangriffe – Betrifft mich das?

Cyberangriffe auf Unternehmen, Verwaltungen und Privatnutzer kommen jeden Tag vor. Viele Angriffe sind erfolgreich, weil die Täter immer professioneller werden; allzu oft wird es ihnen aber auch unnötig leicht gemacht. Die zunehmende Vernetzung der IT-Systeme ermöglicht Angriffe aus der Ferne von nahezu jedem Ort der Welt. Die Gefahr, entdeckt und zur Rechenschaft gezogen zu werden, ist gering.

Die immer rascher fortschreitende Digitalisierung und Vernetzung vieler Lebens- und Arbeitsbereiche führt zu einer dynamischen Gefährdungslage. Die Verbindung von privater und beruflicher Nutzung mobiler Endgeräte mit Zugang zum Firmennetz vergrößert die Möglichkeiten für Cyberkriminelle, auf Unternehmensdaten zuzugreifen. Durch die zunehmende Digitalisierung der Wirtschaft (Industrie 4.0) und die Durchdringung des Privatlebens mit digitalen Funktionen (Smart Living) steigt auch die Verwundbarkeit der Systeme durch Cyberattacken und führt zu völlig neuen Herausforderungen für Cybersicherheit und -abwehr.

In den vergangenen Jahren sind die Bedrohungslage und die Gefährdung von Privatnutzern, Unternehmen und staatlichen Einrichtungen deutlich gestiegen. Durch die Veröffentlichungen des Whistleblowers Edward Snowden und die immer häufigeren Medienberichte über spektakuläre Cyberangriffe und Datendiebstähle erhält die Öffentlichkeit zunehmend eine Vorstellung von dem enormen Bedrohungspotential. Die Einblicke in die technischen Möglichkeiten von Cyberkriminellen, die Professionalität staatlich gelenkter Cyberspionage und die riesigen Schadenssummen erschüttern immer mehr das Vertrauen in die Sicherheit der IT-Nutzung. Beispiele sind der im Mai 2015 bekannt gewordene Angriff auf den Deutschen Bundestag, der digitale Bankraub einer Bande („Carbanak/Anunak“) bei 100 osteuropäischen Finanzinstituten mit einem Schaden von einer Milliarde US-Dollar, durch Kryptotrojaner bedingte IT-Ausfälle bei Behörden, Krankenhäusern und der Bahn sowie der Ausfall von fast einer Million DSL-Routern im November 2016 in Deutschland durch einen weltweiten Cyberangriff.

Das Dunkelfeld bei Cybercrime ist groß. Viele Straftaten werden entweder überhaupt nicht entdeckt oder nicht angezeigt.

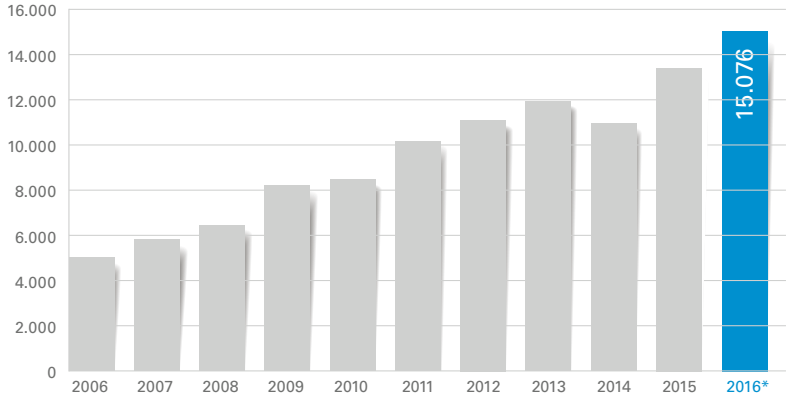
4.2 Wie viele Cyberstraftaten werden der Polizei bekannt?

Für das Jahr 2016 registrierte die Polizeiliche Kriminalstatistik (PKS) in Bayern insgesamt 15.076 Straftaten im Bereich Cyberkriminalität im engeren Sinne mit einem Gesamtschaden von 10,5 Millionen Euro. Hiervon entfielen über zwei Drittel der Straftaten auf Computerbetrug und Datenausspähung.

Unter Nutzung des „Tatmittels Internet" wurden laut PKS im Jahr 2016 insgesamt 24.871 Straftaten in Bayern begangen. Dabei handelt es sich überwiegend um Betrugsdelikte (Anteil: 70,0 %), darunter vor allem der Warenbetrug, also Fälle, bei denen der Täter Waren zum Verkauf über das Internet anbietet, sie jedoch gar nicht oder in minderwertiger Qualität liefert.

Die Aussagekraft der PKS über das Ausmaß der Cyberkriminalität und den Schadensumfang ist aber sehr begrenzt. Es ist von einem äußerst großen Dunkelfeld auszugehen. Ein sehr großer Teil der begangenen Delikte wird von der PKS überhaupt nicht erfasst. Zum einen werden nicht alle Straftaten in der PKS statistisch abgebildet; beispielsweise bleiben im Ausland begangene Straftaten unberücksichtigt. Zum anderen wird ein Großteil der Straftaten im Netz nicht angezeigt, entweder weil Bürger und Unternehmen nicht bemerken, dass sie Opfer von Cyberkriminellen geworden sind oder weil Unternehmen eine negative „Publicity" scheuen.

Polizeilich erfasste Fälle von Cyberkriminalität in Bayern von 2006 bis 2016



* Aufgrund geänderter Verschlüsselungslogik sind einige Deliktsschlüssel und der Summenschlüssel mit den Vorjahren nicht mehr vergleichbar.

4.3 Wie gefährdet bin ich als IT-Nutzer?

› Privatnutzer

Laut einer im Februar 2015 veröffentlichten repräsentativen Studie des Deutschen Instituts für Wirtschaftsforschung (DIW) ist in Deutschland bei Privatpersonen jährlich von 14,7 Millionen Internetdelikten auszugehen. Der finanzielle Schaden in den Bereichen Phishing, Identitätsdiebstahl, Warenbetrug und Schadsoftware beläuft sich hiernach auf jährlich 3,4 Milliarden Euro. Eine Umfrage des Branchenverbandes BITKOM im Jahr 2017 bei rund 1.000 Internetnutzern ergab, dass 49 % der Befragten in den vergangenen 12 Monaten Opfer von Cyberkriminalität geworden sind.

Jeder zweite Internetnutzer in Deutschland war in den vergangenen zwölf Monaten Opfer von Cyberkriminalität.

› Wirtschaft

Die deutsche Wirtschaft ist ein attraktives Ziel für Cyberkriminelle, insbesondere für Cyberspionage und -sabotage. Das Know-how deutscher Unternehmen ist weltweit begehrt. Wirtschaftsspionage und Konkurrenzausspähung richten sich daher vor allem gegen technologieorientierte und innovative Unternehmen, insbesondere auch gegen kleinere und mittelständische Unternehmen, das Rückgrat der deutschen und bayerischen Wirtschaft. Erfolgreiche Spionageangriffe können immense volkswirtschaftliche Schäden verursachen, wenn aus Unternehmen oder Forschungseinrichtungen geistiges Eigentum abfließt. Sabotageakte dienen häufig der Erpressung von Unternehmen, d. h. lahmgelegte oder beschädigte IT-Systeme werden nur gegen Bezahlung hoher Summen wiederhergestellt.

65,6 % der Unternehmen und Behörden waren in den vergangenen zwei Jahren Ziel von Cyberangriffen. In nahezu der Hälfte (47 %) der Fälle waren die Angreifer erfolgreich. Zu diesem Ergebnis kommt die im Oktober 2016 veröffentlichte Cybersicherheits-Umfrage des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die im Juli 2017 veröffentlichte Studie des Branchenverbandes BITKOM kommt zu vergleichbaren Ergebnissen: Hiernach sind 53 % aller Unternehmen in Deutschland in den vergangenen zwei Jahren Opfer von Datendiebstahl, digitaler Wirtschaftsspionage oder -sabotage geworden. Die am stärksten gefährdeten Wirtschaftszweige sind der Automobil- und Maschinenbau und die Luft- und Raumfahrttechnik, gefolgt von der Chemie- und Pharmabranche und den Finanzinstituten.

Der Schaden für die gesamte deutsche Wirtschaft beläuft sich auf rund 55 Milliarden Euro jährlich. Dabei sind die mittelständischen Unternehmen am stärksten betroffen (61 %). Für Mittelständler kann eine Cyberattacke existenzgefährdend sein. Das zeigen die in der „E-Crime-Studie 2017“ von der Wirtschaftsberatungsgesellschaft KPMG ermittelten Schadenssummen zwischen 15.000 und 150.000 Euro je Fall bei der Mehrheit der befragten Unternehmen. In Einzelfällen lag der Gesamtschaden über eine Million Euro. Bei der Verletzung von Geschäfts- und Betriebsgeheimnissen oder Urheberrechtsverletzungen liegen die Schadenssummen sogar noch deutlich höher.

Fast 55 Milliarden Euro Schaden pro Jahr* (Basis: Selbsteinschätzung aller befragten Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=571))

Delikttyp	Schadenssummen (€)
Kosten für Ermittlungen und Ersatzmaßnahmen	21,1 Mrd.
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	17,1 Mrd.
Patentrechtsverletzungen (auch schon vor der Anmeldung)	15,4 Mrd.
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	15,4 Mrd.
Kosten für Rechtsstreitigkeiten	11,0 Mrd.
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	10,5 Mrd.
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	6,9 Mrd.
Datenschutzrechtliche Maßnahmen (z. B. Information von Kunden)	6,4 Mrd.
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	1,3 Mrd.
Sonstige Schäden	4,5 Mrd.
Gesamtschaden innerhalb der letzten zwei Jahre	**109,6 Mrd.**

*Schäden in Deutschland

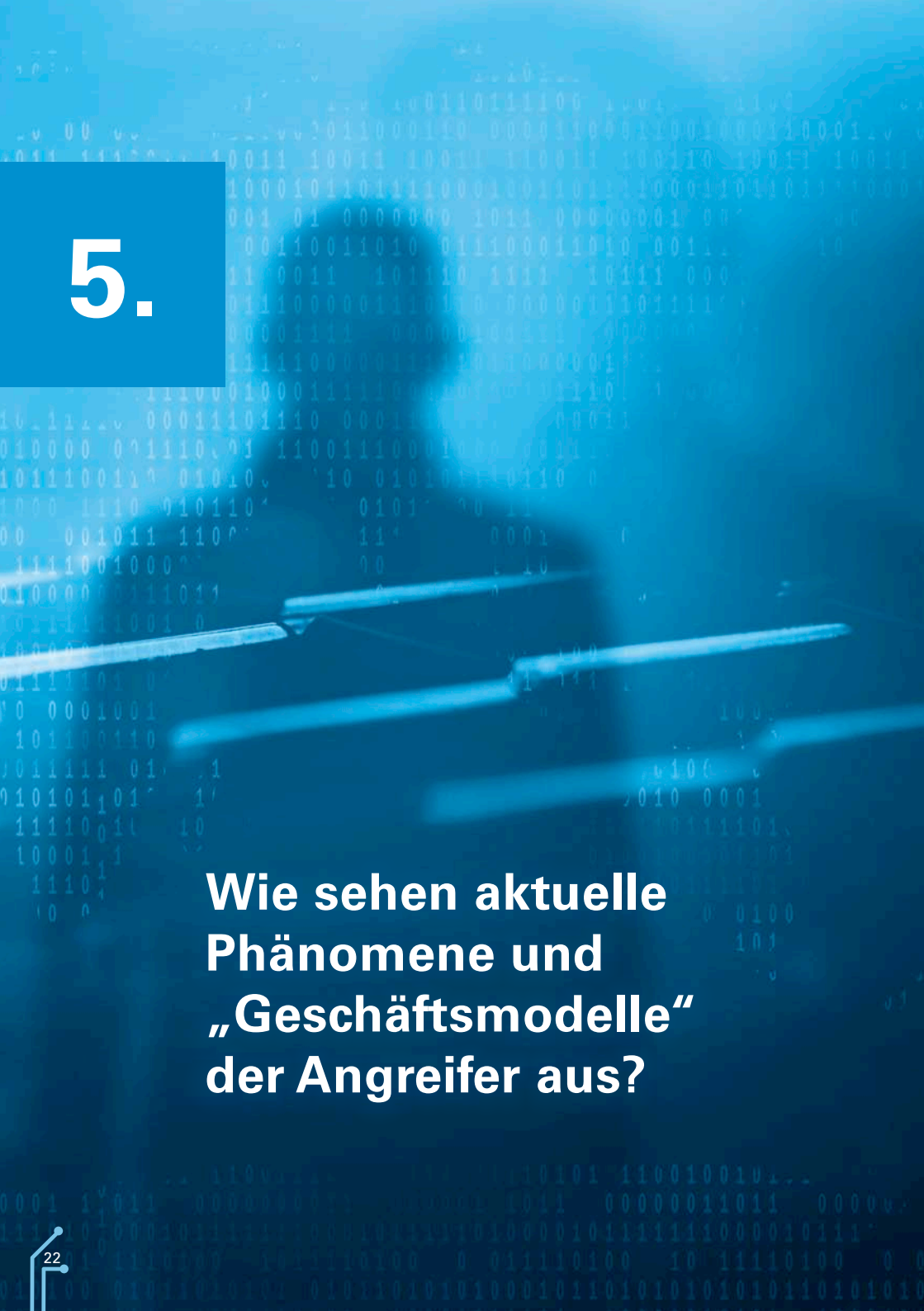
› Betreiber Kritischer Infrastrukturen

Auch kritische Infrastrukturbetriebe bleiben von gezielten IT-Angriffen nicht verschont. Kritische Infrastrukturen sind „zentrale Nervensysteme“ unserer hochentwickelten Gesellschaft. Darunter versteht man Einrichtungen mit wichtiger Bedeutung für das Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (z. B. Kraftwerke, Trinkwasserversorgung). Die verlässliche Bereitstellung der Dienstleistungen dieser Infrastrukturen ist eine Grundvoraussetzung für die wirtschaftliche Entwicklung, das Wohlergehen unserer Gesellschaft und für politische Stabilität.

Das von Kritischen Infrastrukturen ausgehende Bedrohungspotential für die Innere Sicherheit ist enorm. Da es bei deren Ausfall oder Beeinträchtigung zu Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen kommen kann, bedürfen sie besonderen Schutzes. Dies belegt z. B. der durch einen Cyberangriff mit dem Schadprogramm „Black Energy“ ausgelöste Stromausfall am 23.12.2015 in der Ukraine.

Spionage- und Sabotageakte richten sich besonders oft gegen mittelständische Unternehmen. Ein Cyberangriff kann für sie existenzbedrohend sein.

5.



Wie sehen aktuelle Phänomene und „Geschäftsmodelle“ der Angreifer aus?

5. Wie sehen aktuelle Phänomene und „Geschäftsmodelle“ der Angreifer aus?

Im besonderen Fokus der Angreifer stehen die Betriebssysteme Windows und Android.

› Schadprogramme

Bei der Begehung von Straftaten im Bereich Cyberkriminalität spielen Schadprogramme nach wie vor die zentrale Rolle. Laut BSI gab es im Herbst 2016 weltweit über 560 Millionen Schadprogrammvarianten. In Deutschland gibt es jeden Monat mindestens eine Million Infektionen durch Schadprogramme, wobei sich der Fokus der Cyberkriminellen zunehmend auf die Programmierung von Schadprogrammen für mobile Endgeräte (Smartphones, Tablets) richtet.

Anfang 2016 war Deutschland von einer massiven Welle von Ransomware-Infektionen betroffen („Wannacry“, „NotPetya“). Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese nur gegen Zahlung eines Lösegeldes („ransom“) wieder freigeben. Beim überwiegenden Teil der Angriffe handelt es sich um ungezielte Massenangriffe, die z. B. über Anhänge von Spam-E-Mails verbreitet werden.

› Diebstahl und Missbrauch digitaler Identitäten

Digitale Identitäten sind ein begehrtes Diebesgut von Cyberkriminellen. Als Identitätsdiebstahl oder -missbrauch bezeichnet man die Aneignung bzw. unberechtigte Nutzung personenbezogener Daten wie Anschrift, E-Mail-Adresse, Geburtsdatum, Bankkonto- oder Kreditkartennummern. Ziel des Angreifers ist es, entweder die erlangten Informationen für eigene kriminelle Zwecke einzusetzen oder die gestohlenen Daten über illegale Verkaufsplattformen global zum Kauf anzubieten. Das bekannteste Phänomen des Identitätsdiebstahls ist das sog. Phishing im Zusammenhang mit Onlinebanking. Die Täterseite ist jederzeit in der Lage, neue Schadsoftware zu entwickeln, um die gesicherten Transaktionsverfahren zu umgehen.

› Botnetze und DDoS-Angriffe

Ferngesteuerte Botnetze spielen weiter eine große Rolle. Das IoT-Botnetz „Mirai“ hat 2016 die Bedrohung, die in diesem Zusammenhang vom Internet der Dinge ausgeht, verdeutlicht. Botnetze konnten aber

Deutsche Regierungsnetze werden im Schnitt alle zwei Tage von ausländischen Nachrichtendiensten angegriffen.

auch schon erfolgreich bekämpft werden: Im Februar 2015 hat das BKA den in Deutschland gehosteten Teil des „Ramnit-Botnetzes“ mit weltweit ca. 3,2 Millionen Computersystemen deaktiviert. Durch Unterstützung des BSI konnten Ende 2016 zudem Teile der weltweiten Botnetz-Infrastruktur „Avalanche“ zerschlagen werden.

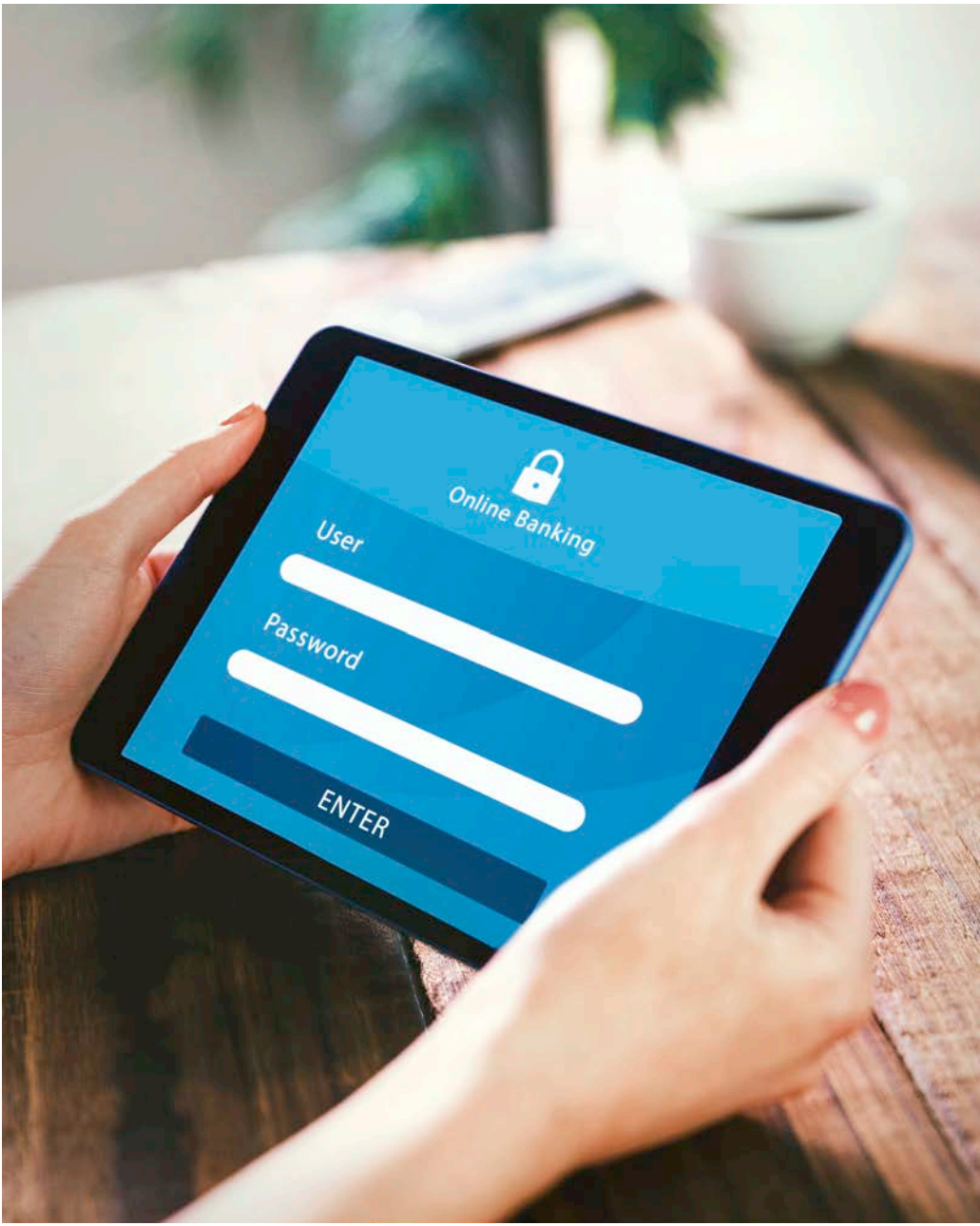
Eng verknüpft mit dem Thema Botnetze sind die sog. DDoS-Angriffe. Auch DDoS-Angriffe werden immer umfangreicher und raffinierter. Die Motive der Täter reichen von politischen Zielen über die Erlangung von Wettbewerbsvorteilen bis hin zur Geldbeschaffung mittels Erpressung. DDoS-Angriffe können für wenig Geld (ca. 500 US-Dollar) auf dem Schwarzmarkt in Auftrag gegeben werden. Für die Betroffenen können die Auswirkungen existenzvernichtend sein, da beispielsweise die Kunden eines Online-Shops schnell zur Konkurrenz wechseln, wenn die Firma online nicht mehr erreichbar ist.

› APT-Angriffe

APT-Angriffe kommen vornehmlich im Bereich Cyberspionage und -sabotage zum Einsatz und sind eine ernstzunehmende Bedrohung für die deutsche Wirtschaft wie auch für staatliche Stellen. Konkrete Zahlen liegen hierzu nicht vor, da die Angriffe nur selten öffentlich bekannt werden. Betroffen sind insbesondere die Branchen Rüstung, Raumfahrt, Maschinenbau und Forschungseinrichtungen. Der Angriff beginnt häufig mit zielgerichtetem Social Engineering, gefolgt von der Versendung einer personalisierten mit Schadsoftware präparierten E-Mail.

› Cybercrime-as-a-Service

Ein aktuelles Phänomen ist das Geschäftsmodell „Cybercrime-as-a-Service“, das immer mehr an Bedeutung gewinnt. Die Entwickler einschlägiger Schadsoftware wenden diese heute oft nicht mehr selbst an, sondern bieten sie in der „Underground Economy“ weltweit zum Verkauf an (z. B. Bereitstellung von Botnetzen, DDoS-Attacken). Kriminelle können damit auch ohne eigene IT-Kenntnisse alle Formen von Cyberattacken ausführen, was das Gefährdungspotential zusätzlich erhöht. Auch die Organisierte Kriminalität wird im Bereich Cybercrime zunehmend aktiv.


Online Banking
User
Password
ENTER

6.

Wie schützt der Freistaat Bayern Staat, Bürger und Wirtschaft vor Cybergefahren?

Initiative Cybersicherheit Bayern

6. Wie schützt der Freistaat Bayern Staat, Bürger und Wirtschaft vor Cybergefahren?

Cybersicherheit ist eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft. Der Staat hat dabei eine wichtige Schutzfunktion.

6.1 Bayerische Cybersicherheitsstrategie

Die Verfügbarkeit des Cyberraums und der Schutz der darin vorhandenen Daten sind in unserer zunehmend vernetzten Welt zu einer existenziellen Frage des 21. Jahrhunderts geworden. Deshalb ist es eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft, für ein hohes Maß an Cybersicherheit zu sorgen. Die Gewährleistung von Cybersicherheit ist zu einem zentralen Querschnittsthema der Inneren Sicherheit geworden, das alle Gesellschaftsbereiche angeht. Auch wenn die primäre Verantwortung für die Sicherheit der eigenen Daten und die Integrität der eigenen IT-Systeme beim jeweiligen Nutzer liegt, kommt dem Staat eine Schutzfunktion zu.

Um dieser Verantwortung im Freistaat Bayern gerecht zu werden, hat Staatsminister Joachim Herrmann im April 2013 die Bayerische Cybersicherheitsstrategie auf den Weg gebracht. Mit dem ressortübergreifenden Konzept sollen die staatliche Handlungsfähigkeit geschützt und die Sicherheitsbehörden gestärkt werden. Im Fokus stehen zudem der Schutz der Wirtschaft vor Cyberspionage und -sabotage sowie der Schutz der Bürgerinnen und Bürger durch Beratung und Sensibilisierung. Mit der Strategie werden alle für die Cybersicherheit relevanten Akteure unter der ressortübergreifenden Koordination im Bayerischen Staatsministerium des Innern und für Integration vernetzt. Die Cybersicherheitsstrategie setzt auf eine partnerschaftliche Kooperation zwischen Staat, Wirtschaft und Wissenschaft.

In den folgenden vier Haupthandlungsfeldern arbeiten die Verantwortlichen eng zusammen:

- Schutz der öffentlichen IT
- Effektive Bekämpfung der Cyberkriminalität
- Schutz der Wirtschaft vor Spionage und Sabotage
- Datenschutz – Bürger sicher im Netz.

Ergänzend wurde der Ressortkreis „Strategie für Cybersicherheit“ als Netzwerk staatlicher Stellen eingerichtet. Hier werden Informationen ausgetauscht, Aktivitäten koordiniert und ressortübergreifende Projekte zum Thema Cybersicherheit auf den Weg gebracht.

Das Internet darf kein rechtsfreier Raum sein. Die Bayerische Polizei ist für die Bekämpfung der Cyberkriminalität gut gerüstet.

6.2 Bekämpfung der Cyberkriminalität

Die Bayerische Polizei hat sich auf die neue Art der Bedrohung eingestellt. Beim Bayerischen Landeskriminalamt (BLKA) wurde mit dem Dezernat 54 eine Zentralstelle zur Bekämpfung der Cyberkriminalität geschaffen. Es ist erster Ansprechpartner für nationale und internationale Polizeibehörden, für komplexeste Ermittlungen bei Cyberdelikten ausgerüstet und bearbeitet bayernweit Straftaten von erheblichem Umfang oder mit internationalen Bezügen.

Die Zentrale Ansprechstelle Cybercrime (ZAC) ist beim BLKA als zentraler Ansprechpartner der Bayerischen Polizei für alle bayerischen Unternehmen, Behörden, Verbände und sonstigen Institutionen angesiedelt. Als kompetenter Partner ist die ZAC nicht nur „Ersthelfer" und Berater für von Cyberkriminalität betroffene Stellen („single point of contact"), sondern berät interessierte Stellen auch präventiv. Dabei ist der diskrete Umgang mit Informationen – wie für die gesamte Bayerische Polizei – eine gesetzliche Verpflichtung.

Die Bearbeitung schwerer und mittelschwerer Cyberdelikte liegt in ganz Bayern in den Händen der zum März 2017 neu geschaffenen Kommissariate „Cybercrime" bei jeder Kriminalpolizeiinspektion und den Kriminalfachdezernaten bzw. -kommissariaten in München, Nürnberg und Augsburg. Die Bearbeitung von einfach gelagerten Fällen ist Aufgabe der Polizeiinspektionen. Egal wo und wer in Bayern Oper eines Cyberangriffs wird, jeder Bürger findet in seiner unmittelbaren Umgebung einen kompetenten Ansprechpartner.

Auch personell ist die Bayerische Polizei für die Bekämpfung der Cyberkriminalität gut gerüstet. Neben den Ansprechpartnern bei allen Polizeiinspektionen sind mittlerweile über 300 Spezialisten in diesem Bereich eingesetzt. Im Rahmen der Sonderlaufbahn „Technischer Computer- und Internetkriminaldienst" werden studierte Informatiker/innen eingestellt und innerhalb eines Jahres zum Polizeivollzugsbeamten weitergebildet. Von den genannten 300 Spezialisten unterstützen 65 ausgebildete IT-Kriminalisten die bayerischen Polizeiverbände bei der Bearbeitung der einschlägigen Kriminalfälle. Zusätzlich wurden im Jahr 2017 rund 70 IT-Kriminalisten eingestellt, die nach der einjährigen Ausbildung im Jahr 2018 auf den Dienststellen zur Verfügung stehen werden.

Um schnell und zielgerichtet auf neue Entwicklungen im Bereich Cybercrime reagieren zu können, investiert die Polizei gezielt in die

Ausstattung hochmoderner Cyberlabore und arbeitet permanent an der Optimierung ihrer strategischen Ausrichtung.

6.3 Schutz der Wirtschaft vor Cyberspionage und -sabotage

Das Cyber-Allianz-Zentrum Bayern (CAZ) beim Bayerischen Landesamt für Verfassungsschutz (BayLfV) ist zentraler, vertraulicher und kompetenter Ansprechpartner für Unternehmen, Hochschulen und Betreiber kritischer Infrastrukturen (KRITIS), wenn es um elektronische Angriffe mit Spionage- oder Sabotagehintergrund geht. Es berät Unternehmen, Hochschulen und KRITIS-Betreiber, wie sie sich mit präventiven Maßnahmen gegen elektronische Angriffe wappnen können, bzw. was zu tun ist, wenn ein Angriff oder Angriffsversuch festgestellt wurde.

Das CAZ garantiert absolute Vertraulichkeit bei Meldungen über mögliche Angriffe, die freiwillig sind und nicht auf gesetzlichen Meldepflichten beruhen. Die Entscheidung, ob im konkreten Fall die Polizei zur Strafverfolgung eingeschaltet werden soll, trifft alleine der Unternehmer. Das BayLfV ist nicht verpflichtet, Straftaten anzuzeigen. Vertraulichkeit ist ein wichtiges Anliegen vieler Unternehmen, die bei Bekanntwerden erfolgreicher Cyberangriffe Reputationsverlust und damit verbundene wirtschaftliche Folgen befürchten.

Die Zusammenarbeit mit dem CAZ bringt für die Unternehmen einen echten Mehrwert: Der Angriff wird von Experten forensisch-technisch analysiert und nachrichtendienstlich bewertet. In die Bewertung fließen Erkenntnisse des Bundesamtes für Verfassungsschutz (BfV) und des BSI ein. Anhand der Rückmeldung können Betroffene das Gefahrenpotential eines Angriffs besser einordnen, das Ergebnis einer eigenen Risikoanalyse unterziehen und gegebenenfalls Organisationsstrukturen anpassen.

Das CAZ steht für:
- **garantierte Vertraulichkeit**
- **schnelle und qualifizierte Rückmeldung**
- **klare Ansprechpartner**

Die technischen Informationen zu einem Angriff gibt das CAZ anlassbezogen und in anonymisierter Form auch an andere potentiell Betroffene weiter, damit auch diese geeignete Schutzmaßnahmen ergreifen können. Über das BfV und die Landesämter für Verfassungsschutz werden die Warnmeldungen an Unternehmen im ganzen Bundesgebiet verteilt.

Das Angebot des CAZ wird von der bayerischen Wirtschaft sehr gut angenommen. Die Warnmeldungen des CAZ zu aktuellen Vorfällen und zum Vorgehen ausländischer Nachrichtendienste werden immer stärker nachgefragt.

7.

Wohin kann ich mich wenden?

7. Wohin kann ich mich wenden?

7.1 Ansprechpartner für Privatanwender

Ansprechpartner für Bürgerinnen und Bürger im Fall eines Cyberangriffs sind in erster Linie die örtlichen Polizeiinspektionen. Sie nehmen den Vorgang auf und geben ihn an die zuständige Polizeibehörde weiter.

Darüber hinaus erhalten Bürgerinnen und Bürger dort Auskunft über die zahlreichen Beratungs- und Präventionsangebote der Polizei zum Thema Cybercrime und Cybersicherheit. Sie erhalten praktische Hinweise zu konkreten Sicherheitsmaßnahmen, um ihren PC oder ihr Smartphone zu schützen und die Gefahren aus dem Netz zu verringern.

Die primäre Verantwortung für die Sicherheit Ihrer Daten liegt bei Ihnen. Informieren Sie sich!

Beratungsangebote der Polizei im Internet:

- Polizeiliche Kriminalprävention der Länder und des Bundes
  www.polizei-beratung.de
- Bayerische Polizei – Beratung
  www.polizei.bayern.de

Kompetente Ansprechpartner für die bayerische Wirtschaft: ZAC und CAZ behandeln Ihre Informationen und Fragen stets diskret und vertraulich.

7.2 Ansprechpartner für Unternehmen

Die Zentrale Ansprechstelle Cybercrime – ZAC – beim Bayerischen Landeskriminalamt ist im Bereich der Strafverfolgung von Cybercrime der zentrale Ansprechpartner bei der Bayerischen Polizei für Unternehmen, Verbände, Behörden und sonstige Institutionen. Sie nimmt Anzeigen entgegen, erledigt gegebenenfalls nötige Sofortmaßnahmen und schaltet bei Bedarf die weiteren Fachdienststellen ein. Die ZAC nimmt im Rahmen der Strafverfolgung eine Vermittler- und Beraterrolle ein. Zudem berät die ZAC Unternehmen und Behörden auch im Vorfeld und klärt, z. B. im Rahmen von Vorträgen oder Beratungsgesprächen, über Präventionsmöglichkeiten, aktuelle Phänomene und vieles mehr auf.

Kontakt

› Bayerisches Landeskriminalamt
Zentrale Ansprechstelle Cybercrime
Maillingerstr.15, 80636 München
Tel.: 089 1212-3300, E-Mail: zac@polizei.bayern.de
www.polizei.bayern.de/lka

Bei elektronischen Angriffen mit Spionage- oder Sabotagehintergrund wenden Sie sich an das CAZ beim BayLfV. Das CAZ bearbeitet nicht nur Verdachtsfälle, sondern unterstützt Unternehmen mit einem breiten Präventionsangebot. Dazu gehören die Beratung von Unternehmen, die Sensibilisierung von Management und Mitarbeitern, individuelle Vorträge und Gespräche in Unternehmen/Hochschulen, mit dem Ziel des Aufbaus einer langfristig angelegten Sicherheitspartnerschaft.

Kontakt

› Bayerisches Landesamt für Verfassungsschutz
Knorrstr. 139, 80937 München
Tel.: 089 31201-222, E-Mail: caz@lfv.bayern.de
(verschlüsselte Kommunikation möglich)
www.verfassungsschutz.bayern.de

› Für allgemeine Fragen zu Wirtschaftsspionage und Wirtschaftsschutz steht das BayLfV unter der Tel. Nr. 089 31201-500, E-Mail: wirtschaftsschutz@lfv.bayern.de zur Verfügung.

› Für Führungskräfte und Mitarbeiter von Unternehmen wurde eine eigene Webseite entwickelt. Das Internetportal „Wirtschaftsschutz Bayern“ (www.wirtschaftsschutz.bayern.de) führt durch ein virtuelles Unternehmen, informiert dabei über potentielle Gefahrenlagen sowie Risikofaktoren und bietet Aufklärung zum Thema Wirtschaftsschutz. Dort sind außerdem Fachinformationen in Form von Flyern, Broschüren und Filmbeiträgen abrufbar.

7.3 Ansprechpartner zu Fragen des Datenschutzes im Zusammenhang mit Cyberkriminalität

Je sensibler man mit seinen Daten umgeht, desto weniger Chancen haben Kriminelle im Netz.

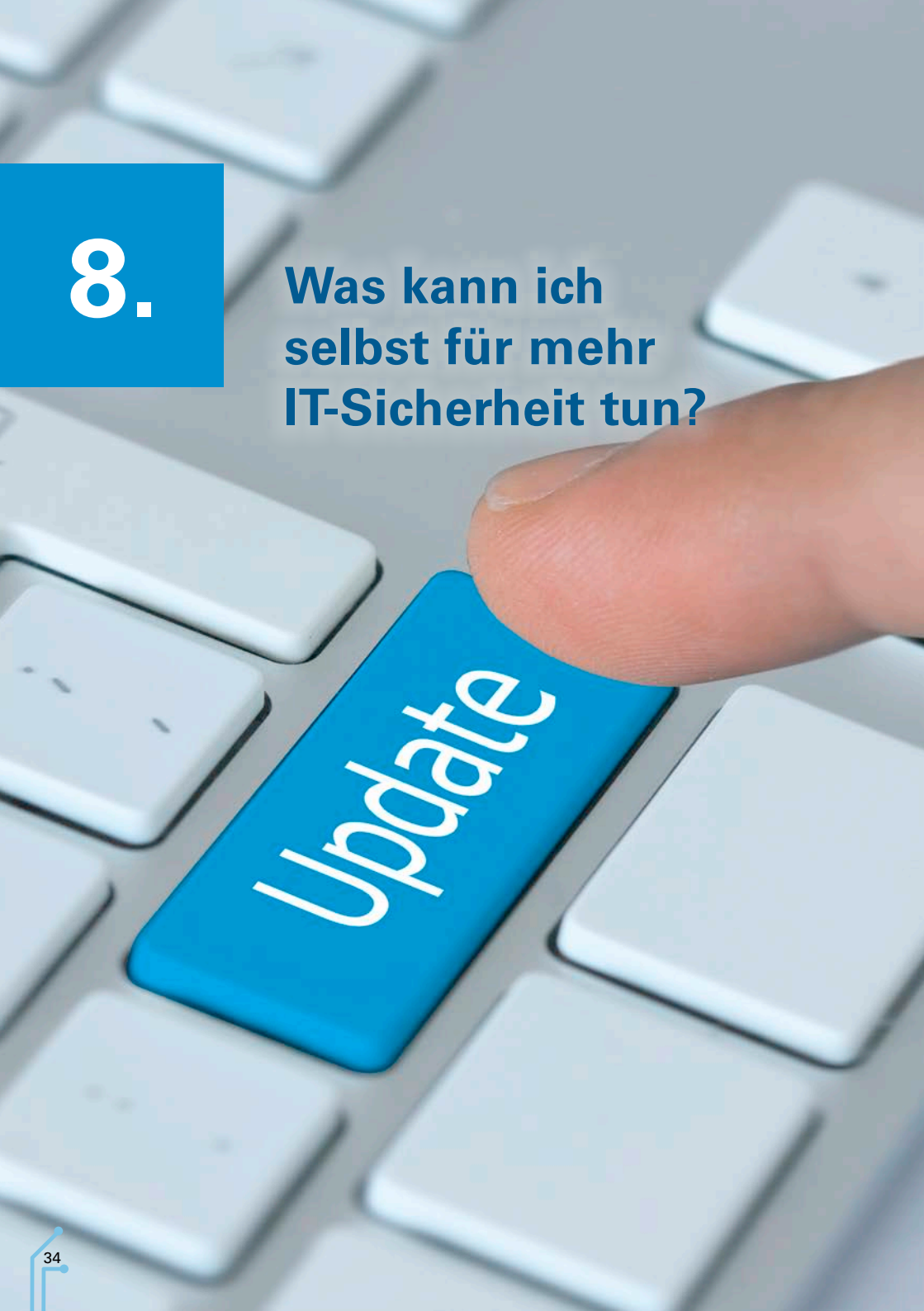
Bei Fragen zum Datenschutz und Beschwerden zu Datenverstößen im Zusammenhang mit Cyberattacken, können sich Bürger und Unternehmen an das Landesamt für Datenschutzaufsicht wenden.

Kontakt

› Landesamt für Datenschutzaufsicht
Promenade 27, 91522 Ansbach
Tel.: 0981 53-1300, E-Mail: poststelle@lda.bayern.de
www.lda.bayern.de

Das Landesamt hat sich deutschlandweit zu einem anerkannten Kompetenzzentrum für Datenschutzfragen im Umgang mit Unternehmen und sozialen Netzwerken entwickelt und bietet auf seiner Homepage umfangreiche Informationen zum Thema „Schutz personenbezogener Daten“ an.

8. Was kann ich selbst für mehr IT-Sicherheit tun?



8. Was kann ich selbst für mehr IT-Sicherheit tun?

100%igen Schutz gibt es nicht, mit relativ geringem Aufwand kann man aber schon ein hohes Maß an Sicherheit erreichen.

8.1 Sicherheitstipps für Privatanwender

Viele Computer von Privatanwendern, die zur Internetnutzung verwendet werden, sind nicht ausreichend gegen die Cybergefahren geschützt. Zwar gibt es keinen hundertprozentigen Schutz gegen diese Gefährdungen. Mit wenigen einfachen Maßnahmen können die Risiken aber deutlich verringert werden. Die nachfolgenden Empfehlungen basieren auf Veröffentlichungen des BSI. Die ersten fünf Empfehlungen („Kernmaßnahmen") sollten Sie in jedem Fall umsetzen. Die weiteren Empfehlungen sind ergänzende Maßnahmen, mit denen Sie Ihre Internet-Sicherheit verbessern und mögliche negative Folgen von Cyberangriffen mindern können. Alle Maßnahmen sind in der Regel auch für Laien einfach umzusetzen. Wenn Sie sich dies dennoch nicht zutrauen, dann sollten Sie einen Internet-Profi oder den Hersteller Ihres IT-Systems zur Rate ziehen, der Sie dabei unterstützen kann.

Die fünf wichtigsten Kernmaßnahmen sind:

- Installieren Sie regelmäßig von den Herstellern bereitgestellte Sicherheitsupdates für Ihr Betriebssystem und die von Ihnen installierten Programme (z. B. Internet-Browser, Adobe Reader) – idealerweise über die Funktion „Automatische Updates". Diese Funktion können Sie in der Regel im jeweiligen Programm einstellen, meist unter dem Menüpunkt „Optionen" oder „Einstellungen".
- Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig, idealerweise über die Funktion „Automatische Updates".
- Verwenden Sie eine Personal Firewall. Diese ist in den meisten modernen Betriebssystemen bereits integriert und soll Ihren Rechner vor Angriffen von außen schützen
- Nutzen Sie für den Zugriff auf das Internet ausschließlich ein Benutzerkonto mit eingeschränkten Rechten, keinesfalls ein Administrator-Konto. Alle gängigen Betriebssysteme bieten die Möglichkeit, sich als Nutzer mit eingeschränkten Rechten anzumelden.

› Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen und Daten. Seien Sie misstrauisch. Klicken Sie nicht automatisch auf jeden Link oder Dateianhang, der Ihnen per E-Mail gesendet wird. Fragen Sie im Zweifelsfall beim Absender nach.

Quelle: www.bsi-fuer-buerger.de

Weitere Empfehlungen und ergänzende Maßnahmen:

› Verwenden Sie einen aktuellen Internet-Browser mit fortschrittlichen Sicherheitsmechanismen. Aktivieren Sie die Sicherheitseinstellungen Ihres Browsers (u. a. „privater Modus", „Verlauf löschen", „Cookies nicht für Drittanbieter zulassen"), um die Speicherung vertraulicher Informationen zu verhindern bzw. zu verringern.

› Nutzen Sie möglichst sichere Passwörter. Verwenden Sie für jeden genutzten Online-Dienst (z. B. E-Mail, Online-Shops, Online-Banking, soziale Netzwerke) ein anderes, sicheres Passwort. Ändern Sie diese Passwörter regelmäßig. Ändern Sie umgehend vom Anbieter oder Hersteller voreingestellte Passwörter.

› Übertragen Sie persönliche Daten (z. B. beim Online-Banking, Online-Shopping) ausschließlich über eine verschlüsselte Verbindung, beispielsweise durch die Nutzung des sicheren Kommunikationsprotokolls „HTTPS".

› Deinstallieren Sie nicht benötigte Programme. Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.

› Erstellen Sie regelmäßig Sicherheitskopien Ihrer Daten, um vor Verlust geschützt zu sein.

› Nutzen Sie nur WLAN („Wireless LAN", drahtloses Netzwerk), das mittels des Standards WPA2 verschlüsselt ist.

› Überprüfen Sie regelmäßig den Sicherheitsstatus Ihres Computers.

8.2 Informationssicherheit in Unternehmen

Informationssicherheit ist kein Produkt, sondern muss gelebt werden.

Wirksamen Schutz vor elektronischen Angriffen bietet ein Informationssicherheits-Managementsystems (ISMS). Darunter versteht man eine Aufstellung von Verfahren und Regeln, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern.

Derzeit gibt es drei Verfahren, die die Mindestanforderungen an ein ISMS gemäß der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrates erfüllen: IT-Grundschutz des BSI, ISO 2700x und ISIS12, ein gegenüber dem BSI-Grundschutz aufwandreduziertes ISMS für kleine und mittelgroße Behörden und Unternehmen (KMU).

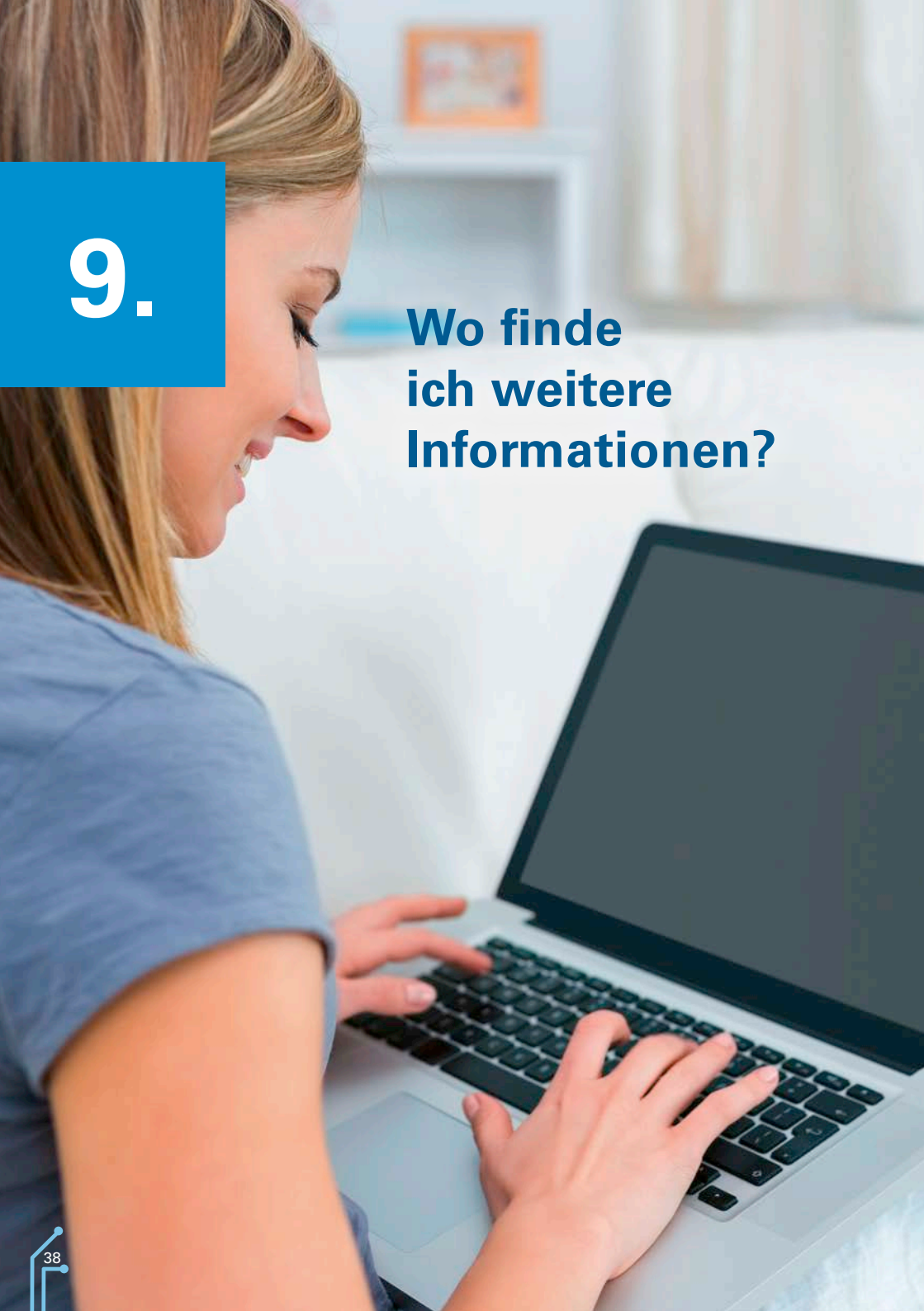
Informationssicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich niemals wieder ändert. Vielmehr erfordern es die ständigen dynamischen Veränderungen, Sicherheit aktiv zu managen, um ein einmal erreichtes Sicherheitsniveau dauerhaft aufrechtzuerhalten. Die Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit ist damit kein statisches Projekt, sondern ein Prozess, in dem das aktuelle Sicherheitsniveau festgestellt und darauf aufbauend Verbesserungen erarbeitet werden.

Beim Aufbau und der Unterhaltung eines ISMS geht es nicht nur um Technik und Organisation, sondern vor allem auch um die Schulung und Sensibilisierung von Mitarbeitern. Nur so kann das für die Schaffung von Informationssicherheit notwendige Sicherheitsbewusstsein entwickelt werden. Denn was hilft die beste Technik, wenn Mitarbeiter z. B. private USB-Sticks auf ihren Arbeitsrechnern verwenden oder manipulierte E-Mail-Anhänge anklicken, ohne sich der damit verbundenen Risiken bewusst zu sein, und damit möglicherweise Schadsoftware in das Netzwerk des Unternehmens gelangen kann.

Die Einführung und Aufrechterhaltung eines ISMS ist Aufgabe der Geschäftsleitung. Dazu gehört auch die Überprüfung, ob die Sicherheitsziele umgesetzt werden. Auch zur Vermeidung von persönlichen Haftungsrisiken ist jeder Unternehmensleitung zu empfehlen, ein IT-Sicherheitsmanagement zu implementieren und für die Mitarbeiter verbindliche Verhaltensregeln festzulegen. Wichtig ist zudem, dass die Geschäftsleitung dem Thema IT-Sicherheit positiv gegenübersteht. Denn nur wenn die Geschäftsleitung hinter den Sicherheitszielen und den damit verbundenen Aktivitäten steht, kann die Aufgabe gelingen.

9.

Wo finde ich weitere Informationen?



9. Wo finde ich weitere Informationen?

- Bayer. Staatsministerium des Innern und für Integration:
  www.cybersicherheit.bayern.de
- Bayer. Staatsministerium für Umwelt und Verbraucherschutz:
  www.vis.bayern.de
- Bayer. Landeszentrale für neue Medien:
  www.blm.de/aktivitaeten/total_digital.cfm
- Bundesamt für Sicherheit in der Informationstechnik:
  www.bsi-fuer-buerger.de und *www.bsi.bund.de*
- Allianz für Cybersicherheit (Initiative des BSI mit dem Digitalverband BITKOM):
  www.allianz-fuer-cybersicherheit.de
- Landeszentrale für Medien und Kommunikation Rheinland-Pfalz:
  www.klicksafe.de
- Initiative „Deutschland sicher im Netz“:
  www.sicher-im-netz.de
- Anti-Botnet Beratungszentrum/ eco-Verband der Internetwirtschaft e.V.:
  www.botfrei.de
- BITKOM E.Learning-Tool Datenschutz:
  www.bitkom-datenschutz.de
- Projekt „Verbraucher sicher online“:
  www.verbraucher-sicher-online.de
- „SCHAU-HIN !“:
  www.schau-hin.info
- Initiative „sicher online gehen“:
  www.sicher-online-gehen.de

Bildnachweis

S. 1	© Leshik/shutterstock.com
S. 4	© BayStMI
S. 6	© everything possible/shutterstock.com
S. 7	© asharkyu/shutterstock.com
S. 9	© everything possible/shutterstock.com
S. 10	© scyther5/shutterstock.com
S. 11	© Mclek/shutterstock.com
S. 12	© leolintang/shutterstock.com
S. 14	© Roobcio/shutterstock.com
S. 15	© Hyena Reality/shutterstock.com
S. 16	© Vadim Georgiev/shutterstock.com
S. 19	© Den Rise/shutterstock.com
S. 21	© Thorsten Schier/fotolia.com
S. 22	© TheaDesign/shutterstock.com
S. 23	© GaudiLab/shutterstock.com
S. 25	© wavebreakmedia/shutterstock.com
S. 26	© Jakub Krechowicz/shutterstock.com
S. 27	© rvlsoft/shutterstock.com
S. 29	© psdesign1/fotolia.com
S. 30	© Boumen Japet/shutterstock.com
S. 31	© Archiv Bayerns Polizei
S. 32	© ktsdesign/shutterstock.com
S. 34	© shutteratakan/shutterstock.com
S. 36	© Lisa S./shutterstock.com
S. 38	© wavebreakmedia/shutterstock.com

Bayern.
Die Zukunft.

IMPRESSUM

Herausgeber	Bayerisches Staatsministerium des Innern und für Integration Odeonsplatz 3, 80539 München
Redaktion	Abteilung Verfassungsschutz, Cybersicherheit
Druck	SCHMID Druck+Medien GmbH, www.druckerei-schmid.de
Konzeption & Design	acm Werbeagentur GmbH, www.acm.de
Stand	April 2018

HINWEIS

Diese Druckschrift wird im Rahmen der Öffentlichkeit der Bayerischen Staatsregierung herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern im Zeitraum von fünf Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Landtags-, Bundestags-, Kommunal- und Europawahlen. Missbräuchlich ist während dieser Zeit insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken und Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die Druckschrift nicht in einer Weise verwendet werden, die als Parteinahme der Staatsregierung zugunsten einzelner politischer Gruppen verstanden werden könnte. Den Parteien ist es gestattet, die Druckschrift zur Unterrichtung ihrer eigenen Mitglieder zu verwenden.

BAYERN | DIREKT
Tel. 089 12 22 20

Wollen Sie mehr über die Arbeit der Bayerischen Staatsregierung erfahren?

BAYERN | DIREKT ist Ihr direkter Draht zur Bayerischen Staatsregierung.

Unter Telefon 089 122220 oder per E-Mail an direkt@bayern.de erhalten Sie Informationsmaterial und Broschüren, Auskunft zu aktuellen Themen und Internetquellen sowie Hinweise zu Behörden, zuständigen Stellen und Ansprechpartnern bei der Bayerischen Staatsregierung.

Die Servicestelle kann keine Rechtsberatung in Einzelfällen geben.

Bayern.
Die Zukunft.