Helmut Reimer

Report

BSI: Diskussionsgrundlage zu Sicherheitsanforderungen für Smartphones

Als Diskussionsgrundlage zur Entwicklung von Sicherheitsanforderungen für Smartphones hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) am 25 Februar 2020 einen Anforderungskatalog veröffentlicht. Damit Anwender sich möglichst sicher in der digitalen Welt bewegen können, listet der Anforderungskatalog Sicherheitskriterien auf, die Smartphones im Auslieferungszustand und darüber hinaus erfüllen sollten. Der Katalog ist Ausgangspunkt für einen öffentlichen Diskurs mit Herstellern und Erstausrüstern (Original Equipment Manufacturer, OEM), Netzbetreibern und Zivilgesellschaft. Das BSI strebt eine Beteiligung aller gesellschaftlichen Gruppen bei der Fortentwicklung dieser Anforderungen an, die zukünftig in Richtlinien für die Erteilung des von der Bundesregierung geplanten IT-Sicherheitskennzeichens für Smartphones einfließen sollen.

„Smartphones haben sich in den letzten Jahren zur Schaltzentrale entwickelt, über die wir immer mehr Alltagsvorgänge steuern und abwickeln. Unsichere Smartphones können somit sehr schnell sehr reale negative Auswirkungen haben. Verbraucherinnen und Verbraucher sollten sich darauf verlassen können, dass ein Smartphone bereits beim Kauf eine Grundausstattung an IT-Sicherheit enthält, so dass sie die Möglichkeiten der Digitalisierung möglichst reibungslos nutzen können. Hersteller und OEM sind daher aufgerufen, die Geräte so sicher zu machen wie möglich, und zwar von Anfang an und über eine gewisse Nutzungsdauer hinweg. Unser Anforderungskatalog ist ein Wegweiser zu mehr Security-by-Design und Security-by-Default", betont BSI-Präsident Arne Schönbohm.

Der Anforderungskatalog des BSI enthält Kriterien zur Absicherung der Geräte durch bestimmte Hardwareeigenschaften sowie zur Härtung und zum Schutz der im Auslieferungszustand enthaltenen Software. Zudem konkretisiert und vereinheitlicht der Katalog Anforderungen zur Bereitstellung von Updates während der Laufzeit der Geräte. Darüber hinaus beinhaltet der Katalog Kriterien zum Schutz von Nutzerdaten, etwa im Bereich der Telemetriefunktionen, sowie für mehr Transparenz für die Verbraucherinnen und Verbraucher.

Der Anforderungskatalog steht in Deutsch und Englisch auf der Webseite des BSI zum kostenlosen Download zur Verfügung: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Herstelleranforderungen-Smartphones.html;jsessionid=9C467FE7A9C22F411C98BEA3468C8152.1_cid341*

Intelligente Stromnetze: BSI veröffentlicht Marktanalyse

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 03. Februar 2020 die Marktanalyse nach dem Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (MsbG) aktualisiert und veröffentlicht. Die Marktanalyse nach § 30 MsbG umfasst den Stand der Umsetzung der BSI-Standards sowie der eichrechtlichen Anforderungen über die Wertschöpfungskette Messeinrichtung, Smart Meter Gateway, Gateway-Administrator und Backendsysteme im Markt.

Die Marktanalyse des BSI hat unter anderem ergeben:

- Die für den sicheren Betrieb intelligenter Messsysteme notwendige Infrastruktur (Smart-Meter-Gateway-Administratoren und Smart-Metering-Public-Key-Infrastruktur) steht vollständig zur Verfügung.
- 39 Unternehmen sind derzeit als Smart-Meter-Gateway-Administrator beim BSI registriert und bieten Dienstleistungen zur Gewährleistung des sicheren Betriebs der intelligenten Messsysteme an.
- Zur Wahrung der Privatsphäre und Vertraulichkeit werden die übermittelten Messwerte der Verbraucherinnen und Verbraucher verschlüsselt und integritätsgesichert. Die hierfür nötigen digitalen Zertifikate werden derzeit von 11 Zertifizierungsdienstleistern angeboten.
- Mit der Anpassung ihrer Prozesse hat die Energiewirtschaft sichergestellt, dass Daten aus den intelligenten Messsystemen empfangen und verarbeitet werden können.
- Aktuell haben drei Smart-Meter-Gateway-Hersteller das Produkt-Zertifizierungsverfahren des BSI erfolgreich abgeschlossen.

Feststellung der technischen Möglichkeit

Die Marktanalyse bildet die Grundlage für die Feststellung der technischen Möglichkeit nach § 30 MsbG durch das BSI, mit der bei Vorliegen aller Voraussetzungen offiziell die Rollout-Verpflichtung der grundzuständigen Messstellenbetreiber beginnt. Die Voraussetzungen zum Einbau von intelligenten Messsystemen sind nun gegeben, da drei Smart Meter Gateways voneinander unabhängiger Hersteller vom BSI zertifiziert wurden und die technische Möglichkeit zum Einbau intelligenter Messsysteme durch das BSI festgestellt wurde. Damit sind grundzuständige Messstellenbetreiber verpflichtet, Stromkunden mit einem Jahresverbrauch von 6.000 kWh bis höchstens 100.000 kWh mit einem intelligenten Messsystem auszustatten. Bei einem Jahresstromverbrauch von weniger als 6.000 kWh ist der Einbau optional und die Entscheidung über einen Einbau liegt beim grundzuständigen Messstellenbetreiber. Messsysteme, die nicht den Anforderungen des BSI entsprechen, dürfen dort nicht mehr verbaut werden. Den Verwaltungsakt zur Feststellung der technischen Möglichkeit stellt das BSI auf seiner Internetseite zur Verfügung. Der Tenor des Verwaltungsaktes wird parallel im Bundesanzeiger veröffentlicht. Das BSI wird die nächste Marktanalyse außerplanmäßig zum 30. Oktober 2020 aktualisieren.

Für Verbraucherinnen und Verbraucher, die sich über die Digitalisierung der Energiewende und das Thema Smart Meter Gateway informieren möchten, stellt das BSI umfassende und leicht verständliche Informationen auf seiner Webseite unter *https://www.bsi-fuer-buerger.de* zur Verfügung.

Fachinformationen zum Thema Smart-Metering sind unter *https://www.bsi.bund.de/SmartMeter* abrufbar.

HmbBfDI: 28. Tätigkeitsbericht 2019

Der am 13. Februar 2020 vorgelegte Tätigkeitsbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) zum Berichtsjahr 2019 gibt sowohl Anlass zurückzublicken als auch eine Standortbestimmung vorzunehmen, um die künftigen Ziele ins Auge fassen zu können. Im Mai werden es zwei Jahre, in denen die Datenschutzgrundverordnung (DSGVO) gültig ist. Durchsetzung und Umsetzung der neuen Regelungen des Datenschutzrechts nehmen in Hamburg und auch in Deutschland insgesamt an Fahrt auf. Gleichzeitig zeigen sich aber auch zum einen negative Auswirkungen der limitierten Behördenressourcen und zum anderen dramatische Unterschiede im europäischen Vollzug.

Datenschutz vor Ort

Moderner Datenschutz ist multifunktional. Die Öffentlichkeit ist für die Risiken und Rechte im Zusammenhang mit der Verarbeitung von Daten zu sensibilisieren. In Staat und Gesellschaft muss das Bewusstsein geschärft werden, dass angesichts einer immer stärkeren Vernetzung und einer immer größeren Abhängigkeit der Wirtschaft und der Verwaltung von der Verarbeitung von Daten die Rechte der Bürgerinnen und Bürger effektiv zu schützen sind. Gleichzeitig gilt es, insbesondere bei jungen Menschen die Kompetenz für den Schutz der eigenen und den Respekt vor den Daten anderer zu fördern. Hier hat der HmbBfDI eine Initiative zum Datenschutz in der Medienbildung aufgenommen, die aktuell mit einem Projekt der Förderung des Themas an Schulen startet.

Mit Hilfe der aufsichtsbehördlichen Instrumente wiederum muss sichergestellt werden, dass die Rechte Betroffener seitens der Daten verarbeitenden Stellen gewahrt werden. Seit Inkrafttreten der DSGVO ist ein dramatischer Anstieg von Beschwerden durch Bürgerinnen und Bürger zu verzeichnen. Allein im letzten Jahr wuchs das Beschwerdeaufkommen beim HmbBfDI um 25%, nachdem im Jahr des Inkrafttretens der DSGVO bereits eine Verdoppelung der Eingabenzahlen erfolgte. Die personelle Aufstockung der Behörde um lediglich zwei Stellen im aktuellen Haushalt bleibt angesichts dieser Entwicklung deutlich hinter den Erforderlichkeiten zurück.

Hierzu Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit: "Das neue Bewusstsein von Bürgerinnen und Bürgern über ihre Datenschutzrechte kann nicht hoch genug veranschlagt werden. Beschwerden geben uns auch wichtige Hinweise auf mögliche strukturelle Datenschutzprobleme. Wenn es jedoch nicht gelingt, mit den derzeitigen Ressourcen die Anfragen in zeitlich halbwegs akzeptablen Zeiträumen zu beantworten, bleibt bei den Betroffenen ein negativer Eindruck beim Thema Datenschutz zurück. Mit zusätzlichem, befristetem Personal ist es zuletzt immerhin gelungen, Eingänge und Ausgänge in etwa in der Waage zu halten. Diese Kräfte müssen verstetigt werden. Zudem machen der stetige Zuwachs von Fällen und die erheblichen Rückstände eine weitere Verstärkung erforderlich."

Datenschutz der zwei Geschwindigkeiten?

Die umfangreichen Sanktionsbefugnisse zur Ahndung von Datenschutzverstößen sind entscheidend für die Durchsetzung von Rechten und Freiheiten Betroffener in einem sich immer schneller drehenden Karussell der Datenkapitalisierung. Leider werden die europaweit harmonisierten Sanktionsinstrumente sehr uneinheitlich umgesetzt.

Je nach Sitz der verantwortlichen Stelle sind unterschiedliche nationale Behörden bei grenzüberschreitenden Datenverarbeitungen federführend für deren gesamte Aktivitäten zuständig (sog. One-Stop-Shop-Verfahren). Hierbei sind Abstimmungsverfahren unter vielen europäischen Aufsichtsbehörden zu bewältigen, einschließlich der Befassung durch den Europäischen Datenschutzausschuss, einem Gremium aller EU-Aufsichtsbehörden. Dies gestaltet sich schwerfällig, zeitaufwändig und ineffektiv und bleibt im Ergebnis häufig enttäuschend. Rechtsverbindliche Maßnahmen gegen global agierende Internetdienste sind auch nach Beschwerden bislang weitgehend ausgeblieben. Damit verbundene Richtungsentscheidungen zur Auslegung der DSGVO liegen auf Eis.

Die Ziele der DSGVO werden so in ihr Gegenteil verkehrt. Statt eines harmonisierten Rechtsvollzugs entsteht ein höchst unterschiedliches und intransparentes Milieu der Vollzugskulturen. Statt Rechtsschutz für betroffene Personen herzustellen, werden Verfahren hinausgeschoben, bis sie nahezu in Vergessenheit geraten. Statt eines fairen Wettbewerbs auf dem gemeinsamen Markt für digitale Dienstleistungen verfestigen sich nationale Biotope für Digitalkonzerne, die ihre Marktstellung in Europa gegenüber anderen Wettbewerbern sichern und ausbauen. Für die Akzeptanz der Datenschutzregeln ist der Eindruck fatal, gerade die großen Marktteilnehmer stünden jenseits der Vorschriften.

Hierzu Johannes Caspar: „Dass gegen die Mehrzahl der global führenden Internetdienstleister und Plattformen seit Geltung der DSGVO trotz zahlreicher Meldungen über Datenschutzverletzungen in den letzten beiden Jahren keinerlei rechtsverbindliche Maßnahmen erlassen wurden, noch nicht einmal Entscheidungsentwürfe dazu vorliegen, ist ein schlechtes Zeichen im Jahr 2 nach Einführung der DSGVO. Unterschiedliche rechtlich-kulturelle Traditionen im Vollzug, fehlende Korrekturmöglichkeiten für untätige federführende Behörden, unterschiedliche nationale Vorschriften zum Verwaltungsverfahren sowie eine Massierung von Unternehmen in wenigen Mitgliedstaaten, zeigen: Das Konzept des One-Stop-Shop mag gut gedacht sein, ist aber nicht praxistauglich.

„Die Defizite sind strukturell und lassen sich aus meiner Sicht allein auf kooperativer Basis zwischen den Aufsichtsbehörden nicht beheben. Es bedarf der rechtlichen Umsteuerung. Die Hoffnung, der Faktor Zeit werde diese Situation heilen, ist trügerisch und verlängert nur den derzeitigen Zustand. Zeit ist die knappste Ressource im Prozess der Digitalisierung. Der Spielball liegt nun im Feld der EU-Kommission, im Rahmen des Ende Mai vorzulegenden Evaluationsberichts geeignete Vorschläge für Rechtsänderungen zu präsentieren. Ein Zuwarten bis zur nächsten Evaluation wäre fatal, denn diese findet turnusgemäß erst 2024 statt."

Die elektronische Fassung des Datenschutz-Tätigkeitsberichts kann hier abgerufen werden: *https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf*

Amtswechsel im BayLDA

Der Bayerische Innenminister Joachim Herrmann hat am 31. Januar 2020 den langjährigen Präsidenten des BayLDA, Thomas Kranig in den Ruhestand verabschiedet. Er bescheinigte ihm, dass er seit dem 1. August 2011 die Geschicke des Landesamtes geleitet, großartige Aufbauarbeit geleistet und eine schlagkräftige und moderne Behörde geformt habe. Er hinterlasse große Fußstapfen. Mit klugen Personalentscheidungen, exzellenter Teamführung und immer wieder auch dem richtigen Gespür für prägende Entwicklun-

gen habe er und seine Mitarbeiter die Bedeutung des Datenschutzes im Alltag der Bürgerinnen und Bürger viel bewusster gemacht.

Die Landesbeauftragte für den Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Helga Block, und der Präsident des Bundesverbandes der Industrie, Prof. Dieter Kempf, anerkannten in ihren Grußworten die Leistungen des BayLDA unter seinem Präsidenten Thomas Kranig, das Datenschutzrecht so zu vollziehen, dass die Vereine und Unternehmen verstehen, dass und was sie zum Schutz der personenbezogenen Daten der betroffenen Personen machen müssen.

In seiner Abschiedsrede verwies Präsident Kranig auch auf eine seiner früheren dienstlichen Arbeitsbereiche und meinte, dass sein schönstes dienstliches Erlebnis ein erfolgreiches Mediationsverfahren, das er zusammen mit einer Kollegin als Gerichtsmediator begleitet habe, gewesen sei, im Zuge dessen sechs gerichtliche Streitverfahren zur Zufriedenheit Beteiligten erledigt wurden.

Er wies darauf hin, dass das BayLDA bei seiner Übernahme aus 11 Personen bestand und bei seinem Abschied nunmehr 33 Planstellen zur Verfügung stehen. Der Arbeitsanfall sei nach wie vor gewaltig. Seine Leitlinie sei gewesen, „dass jede Beratung, die dazu führe, dass ein Datenschutzverstoß nicht begangen werde besser sei als jedes Bußgeld. Er verkenne aber nicht, dass Bußgelder jedenfalls dann, wenn die Beratung nicht mehr helfe, eine sehr große und wichtige auch generalpräventive Bedeutung haben."

Präsident Kranig dankte Innenminister Herrmann dafür, dass er Umschichtungsmöglichkeiten im Rahmen des Haushaltsvollzugs dafür genutzt habe, dem BayLDA in diesem Jahr neun neue Stellen auf Dauer zur Verfügung zu stellen. Seinem Nachfolger und Freund Michael Will wünschte er viel Erfolg und eine glückliche Hand bei allen Entscheidungen die er nun als unabhängiger Präsident werde treffen müssen.

Michael Will bedankte sich für das Vertrauen, ihm die verantwortungsvolle Aufgabe der Leitung des BayLDA zu übertragen: „Aus der langjährigen Zusammenarbeit mit Thomas Kranig weiß ich, dass ich mich auf ein großartiges Team freuen darf. Gemeinsam werden wir uns weiterhin dafür einsetzen, dass sich das neue europäische Datenschutzrecht im Alltag der Unternehmen und Vereine genauso wie im täglichen Leben der Bürgerinnen und Bürger bewährt".

Andreas Sachs, Vizepräsident des BayLDA, wünschte Herrn Kranig im Namen aller Mitarbeiterinnen und Mitarbeitern einen wohlverdienten Ruhestand und bedankte sich für dessen Engagement sowie große Fairness für die Belange des LDA-Teams in Zeiten der enormen Arbeitslast, die die Datenschutzgrundverordnung für die Behörde mit sich brachte.

Sächsischer BfD übernimmt Vorsitz in der deutschen Datenschutzkonferenz

Der Sächsische Datenschutzbeauftragte Andreas Schurig wird 2020 der Konferenz der 18 unabhängigen staatlichen Datenschutzaufsichtsbehörden von Bund und Ländern vorsitzen. Er übernimmt diese Aufgabe vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und Vorsitzenden der Datenschutzkonferenz im Jahr 2019, Prof. Dr. Dieter Kugelmann.

Schurig, Mathematiker und Theologe, hat das Amt des Sächsischen Datenschutzbeauftragten seit 2004 inne. 2009 und 2015 wurde er jeweils mit großer Mehrheit durch den Sächsischen Landtag wiedergewählt. Seine Behörde beschäftigt derzeit rund 30 Bedienstete, die die ca. 180.000 Unternehmen, 29.000 Vereine, 2,2 Millionen Privathaushalte sowie zahlreichen öffentlichen Stellen in Sachsen im Hinblick auf deren Umgang mit personenbezogenen Daten beaufsichtigen.

Die Datenschutzkonferenz beschließt die gemeinsamen Forderungen der Datenschutzbeauftragten an Politik und Unternehmen. Sie stützt sich dabei auf ihre Facharbeitskreise wie „Justiz", „Wissenschaft und Forschung" oder „Beschäftigtendatenschutz".

Schurig wird sein Vorsitzjahr unter das Generalmotto „Informationelle Selbstbestimmung" stellen. „Selbstbestimmung ist immer noch der wichtigste Wert des Datenschutzes. Wir müssen angesichts der Internetgiganten mehr denn je dafür sorgen, dass der Einzelne in freier Selbstbestimmung über die Verwendung seiner Daten entscheiden kann.", so Schurig.
Weitere Infos unter *https://www.datenschutzkonferenz-online.de/*

BSI erkennt Cyber-Sicherheitsstandard für Krankenhäuser an

Neben Einrichtungen anderer Sektoren waren Krankenhäuser und andere medizinische Einrichtungen zuletzt wiederholt Betroffene gravierender IT-Sicherheitsvorfälle. Neben der Bedrohung durch Ransomware-Angriffe standen dabei auch sensible Patientendaten im Mittelpunkt. Am 23. Oktober 2019 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Eignung eines branchenspezifischen Sicherheitsstandards (B3S) festgestellt, mit dem Krankenhäuser ihre IT-Sicherheitsmaßnahmen nach dem Stand der Technik ausrichten können. Vorgelegt wurde der B3S von der Deutschen Krankenhausgesellschaft (DKG).

„Krankenhäuser und viele andere Einrichtungen des Gesundheitswesens tragen in mehrfacher Hinsicht eine besondere Verantwortung für ihre IT-Netzwerke. Der Schutz sensibler Patientendaten muss ebenso zuverlässig gewährleistet sein wie die Versorgung von Patientinnen und Patienten mit Unterstützung modernster Computertechnologie. Vor diesem Hintergrund bietet der branchenspezifische Sicherheitsstandard wichtige Rahmenbedingungen, unter denen die Cyber-Sicherheit im Gesundheitswesen weiter erhöht werden kann. IT-Sicherheitsvorfälle wie der erfolgreiche Ransomware-Angriff auf eine Krankenhaus-Trägergesellschaft in Rheinland-Pfalz müssen der Vergangenheit angehören!", so BSI-Präsident Arne Schönbohm.

Etwas weniger als zehn Prozent der Krankenhäuser in Deutschland sind beim BSI als Kritische Infrastrukturen (KRITIS) im Sinne des IT-Sicherheitsgesetzes registriert. Der nun anerkannte B3S steht auch den vielen kleineren Kliniken, die nicht als KRITIS-Betreiber reguliert sind, zur Verfügung und sollte als Maßstab für die Umsetzung angemessener IT-Sicherheitsmaßnahmen dienen. Alle Klinik-Betreiber sind eingeladen, sich in den Netzwerken des BSI wie UP KRITIS und Allianz für Cyber-Sicherheit zu engagieren, um ihr IT-Sicherheitsniveau auf dem bestmöglichen Stand zu halten.

D-TRUST sichert Zugriffe auf elektronische Patientenakte

Am 18. Februar 2020 erfolgte dazu die Vertragsunterzeichnung zwischen gematik und D-TRUST

Welche Medikamente nimmt ein Patient, welche Vorerkrankungen hat er, wie verliefen frühere Behandlungen? Ab 2021 sollen alle gesetzlich Versicherten eine elektronische Patientenakte (ePA) erhalten, die genau diese Informationen bündelt. Der Zugriff des Versicherten auf die ePA erfolgt mittels der elektronischen Gesundheitskarte (eGK). Doch was passiert bei einem Verlust oder Wechsel der eGK? In diesem Fall muss der Zugriff auf die Akte und die eindeutige Zuordnung von Akte und Versicherten technisch sichergestellt werden – einen Teil dieser Aufgabe übernimmt D-TRUST.

D-TRUST, ein Unternehmen der Bundesdruckerei, wurde von der gematik GmbH beauftragt, den sogenannten Schlüsselgenerierungsdienst 2 (SGD2) für die ePA als Dienst der Telematikinfrastruktur (TI) für die elektronische Gesundheitskarte aufzubauen und zu betreiben. „Als qualifizierter Vertrauensdiensteanbieter in Deutschland sind wir stolz, mit dem Schlüsselgenerierungsdienst einen wesentlichen Beitrag zur Sicherheit und Bereitstellung einer zugelassenen elektronischen Patientenakte zu leisten", sagt Dr. Kim Nguyen, Geschäftsführer der D-TRUST GmbH. Die Einführung der ePA ermöglicht dem Versicherten die Verwaltung seiner persönlichen Gesundheitsdaten, die ihm vom Arzt, seiner Krankenkasse oder seinen Gesundheits-Apps bereitgestellt werden. Dieser Service wird seitens der Krankenkassen über 70 Millionen gesetzlich Versicherten und über 200.000 Leistungserbringern ab 2021 zur Verfügung gestellt.

Hintergrund: Jede ePA wird mit zwei Schlüsseln verschlüsselt. Der erste Schlüssel wird stets bereitgestellt von dem jeweiligen Schlüsselgenerierungsdienst 1 des Herausgebers der entsprechenden elektronischen Gesundheitskarte, also den gesetzlichen Krankenkassen. Der zweite Schlüssel wird alleinig erstellt vom zentralen SGD2 der gematik – von D-TRUST. Während der SGD1 für eine begrenzte Anzahl von Nutzern des jeweiligen Kartenherausgebers zur Verfügung gestellt wird, muss der SGD2 als zentraler Dienst in der TI allen gesetzlich Versicherten für die Bildung des zweiten Schlüsselpaares zur Verfügung stehen.

„Der SGD2 ist für die Sicherheit der ePA zentral notwendig, um einen nutzerkontrollierten Zugriff auf die Akte zu ermöglichen und nimmt damit funktional und organisatorisch eine wichtige Stellung in der TI ein", so Nguyen. Aus diesem Grund und wegen der hohen Zahl von Nutzern bestehen für den SGD2 entsprechend der Spezifikationen der gematik höchste Anforderungen an Verfügbarkeit und Performance.

Bundesdruckerei und D-TRUST sind zudem mit weiteren Diensten und Produkten im E-Health-Bereich tätig, auch im Auftrag der gematik. D-TRUST produziert unter anderem die beiden relevanten Karten für die TI: den elektronischen Heilberufsausweis (eHBA) und den elektronischen Praxisausweis- bzw. Institutionsausweis (SMC-B).

Weitere Informationen zu den E-Health Lösungen der Bundesdruckerei und D-TRUST finden Sie hier: *https://www.bundesdruckerei.de/de/Loesungen/E-Health*

Firewall genugate erhält Zulassung bis VS-NfD

Die Firewall genugate 9.0 des Herstellers genua GmbH hat vom Bundesamt für Sicherheit in der Informationstechnik (BSI) am 12. Februar 2020 die Zulassung für den Einsatz bis zum Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch" (VS-NfD) erhalten. Die genugate ist eine zweistufige Firewall mit Application Level Gateway und Paketfilter, mit der Anwender hochkritische Netzwerk-Übergänge im VS-Bereich absichern können. Die VS-NfD-Zulassung erfolgte in einem Pilotprojekt des BSI zu einem neuen Verfahren, das bereits nach Common Criteria (CC) zertifizierte IT-Sicherheitsprodukte innerhalb weniger Wochen durchlaufen können. genua war an der Einführung des neuen „Integrationsverfahrens" als vom BSI qualifizierter Hersteller für VS-Produkte beteiligt. Die Firewall genugate komplettiert das Lösungsangebot von genua zur sicheren VS-NfD-Kommunikation: Als einziger Hersteller bietet genua zugelassene Firewalls und kann darüber hinaus mit zugelassenen VPN-Appliances, Laptops und Devices für mobile Mitarbeiter alle gängigen Kundenanforderungen erfüllen. Damit ist genua der führende Lösungsanbieter für VS-NfD-Kommunikation in Deutschland.

Aufgrund der neuen Verschlusssachenanweisung (VSA), der zunehmenden Digitalisierung und kurzen Innovationszyklen fragen Behörden und Unternehmen immer mehr VS-NfD-zugelassene IT-Sicherheitslösungen nach. Denn die VSA verlangt jetzt von allen an der VS-NfD-Datenverarbeitung beteiligten Systemen, die Sicherheitsfunktionen zum Schutz von Verschlusssachen implementieren, eine BSI-Zulassung – auch von Firewalls.

genua ist vertrauensvoller Partner im Pilotprojekt zu optimierter Zulassung

Auf die verstärkte Nachfrage hat das BSI mit der Entwicklung optimierter Zulassungsverfahren reagiert. Als Hersteller mit langjähriger Erfahrung bei Produktzulassungen hat genua als vertrauensvoller Partner an dem Pilotprojekt zum neuen Integrationsverfahren mitgewirkt. Hier können Evaluationen aus einer Produktzertifizierung nach Common Criteria (CC) beim BSI nach einer Prüfung auch für die Zulassung verwendet werden. Das spart Aufwand und Zeit, sichert gleichzeitig das hohe Qualitätsniveau des Verfahrens. Die High Resistance Firewall genugate 9.0 ist nach CC vom BSI zertifiziert. „Mit dem neuen Verfahren können VS-NfD-Zulassungen innerhalb weniger Wochen durchgeführt werden, ohne Abstriche bei der Prüftiefe und somit beim Qualitätsniveau. So erreicht das BSI das Ziel, für den VS-Bereich schnell zugelassene State-of-the-Art-Sicherheitslösungen bereitzustellen", sagt Matthias Ochs, Geschäftsführer von genua.

Zweistufige Firewall sorgt für hohe Sicherheit an Schnittstellen

Der Einsatzbereich der Firewall genugate sind hochkritische Netzwerk-Übergänge wie z. B. LAN-Internet. Hier erfüllt die Firewall durch den zweistufigen Aufbau hohe Sicherheitsanforderungen: Ein Application Level Gateway und ein Paketfilter sind zu einer Lösung kombiniert. Das Application Level Gateway analysiert den Dateninhalt, unerwünschte oder gar gefährliche Inhalte werden erkannt und geblockt. Der Paketfilter kontrolliert als zweites Firewall-System zusätzlich formale Kriterien wie Absender-, Empfängeradresse und Protokolltyp. Durch die Zweistufigkeit und die umfassende Inhaltskontrolle bietet die genugate ein höheres Sicherheitsniveau als die einstufigen Firewall-Lösungen anderer Hersteller.

OpenText: Cyber-Sicherheit jenseits der Technologie

Wir tendieren dazu, bei Cyber-Sicherheit zunächst immer in technischen Dimensionen zu denken. Es geht um neue Ransomware-

Attacken mit noch gefährlicheren Algorithmen, Viren, Würmern und Phishing. Das sind aber letztlich nur die Speerspitzen des Angriffs. Cyber-Kriminalität ist heute ein Massenphänomen, das sich auf breite Teile der Gesellschaft auswirkt. Betrachtet man nur die technische Seite, kann man die Bedrohung nicht voll erfassen und dagegen vorgehen. Stattdessen müssen auch übergeordnete Entwicklungen berücksichtigt werden. Jochen Adler, verantwortlich für Partnergeschäft bei OpenText in Deutschland, Österreich und der Schweiz, zeigt drei solcher Faktoren auf:

1. Fehlinformationen

Bewusst gestreut oder zufällig „viral gegangen"; falsche Informationen und Fake News verbreiten sich heute rasend schnell. Aktuell kann man das beispielsweise bezüglich des Corona-Virus beobachten. Dazu sind inzwischen so viele Informationen (und so viele davon falsch) im Umlauf, dass selbst die WHO von einer „Infoepidemie" („infodemic") spricht. Welche Ziele die Urheber der Fake News zum Corona-Virus verfolgen, lässt sich kaum ausmachen, zu komplex ist die Situation und verschiedenste Akteure verfolgen mutmaßlich unterschiedlichste Ziele. Andere Beispiele zeigen aber, dass Falschinformationen ganz bewusst und mit einem ausgearbeiteten Plan eingesetzt werden, um beispielsweise Unsicherheit und Zweifel zu verbreiten und sogar politische Prozesse zu beeinflussen – so geschehen im US-Wahlkampf 2016. Auch wenn der Nachweis schwerfällt, dürfte es auch hierzulande solche Fehlinformationskampagnen bereits geben. Allgemein ist das heute ein Phänomen, mit dem man bei allen Entwicklungen von politischer oder gesellschaftlicher Tragweite rechnen muss. Gefährlich wird das immer dann, wenn Mitarbeiter Fake News glauben, eine Sicherheits- oder Bedrohungslage falsch einschätzen, und sich dadurch zu riskantem oder schädlichem Verhalten hinreißen lassen.

2. Missbrauch persönlicher Informationen

Menschen teilen heute immer mehr über sich im Netz mit. Unsere Daten sind überall, das beginnt bei Fotos und Standortangaben in sozialen Medien und endet bei digitalen Krankenakten. Es gibt Dienste, die die eigene DNA analysieren, um Menschen etwas über ihre Abstammung zu verraten. Aktuell ist auch Gesichtserkennung ein großes Thema in den Medien, bei der letztlich ebenfals biometrische Daten anfallen, beispielsweise die Gesichtsgeometrie betreffend. Alle diese Daten müssen irgendwo gespeichert werden, was natürlich bedeutet, dass sie auch kopiert und damit letztlich „gestohlen" werden können. Dies zu verhindern ist eine große Herausforderung; andererseits muss man auch mit dem Schlimmsten rechnen. Unternehmen müssen dafür sorgen, dass sie nicht durch persönliche Daten ihrer Mitarbeiter verwundbar werden, die diese im Netz preisgegeben haben, oder die Hacker bei schlecht gesicherten Firmen, beispielsweise Zulieferern, gestohlen haben. Wenn zum Beispiel Phishing-Attacken per E-Mail immer ausgefeilter werden, so dient das häufig nicht zuletzt dem sogenannten „social engineering": zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen zu bewegen.

3. Spionage und Sabotage

Bedrohungen für Unternehmen und Organisationen müssen deshalb auch nicht immer von außen kommen. Auch eigene Mitarbeiter können zur Gefahr werden, wenn sie vertrauliche Informationen an Dritte weitergeben. Und das nicht nur, weil sie von Kriminellen leichtgläubig und wider besseren Wissens dazu verleitet werden, sondern auch, wenn sie bewusst und aus eigenem Antrieb handeln. Mitarbeiter können zu einem großen Risiko für Unternehmen und Organisationen werden, beispielsweise im Streit und nach einer Kündigung, wenn es ihnen gelingt, sensible Daten nach draußen zu schleusen. Das ist in den meisten Fällen ein Leichtes für die eigenen Mitarbeiter, die Datenzugriff haben und diese beispielsweise auf Cloud-Speicher kopieren können. Ein besonders drastisches Beispiel ereignete sich im letzten Jahr in Frankreich. Der Polizist, der später einen Anschlag auf die Polizeipräfektur in Paris verübte, hatte im Vorfeld in großem Umfang Daten aus seiner Dienststelle herausgeschmuggelt. Ob und an wen er diese sensiblen Informationen weitergegeben hat, blieb unklar. Es muss ja nicht gleich zu einem terroristischen Anschlage kommen: auch Wettbewerbsverletzungen und Sabotage mit digitalen Mitteln sind inzwischen leider Realität geworden, und Behörden sowie Unternehmen dürfen davor nicht die Augen verschließen. Wer seine Mitarbeitenden jedoch unter Generalverdacht stellt, riskiert den totalen Vertrauensverlust auf beiden Seiten. Hier wird viel Fingerspitzengefühl verlangt – eine Fertigkeit, die viele IT-Spezialisten erst erlernen müssen.

Fazit

Die größten Bedrohungen für die Cyber-Sicherheit sind aktuell keine spezifischen Viren oder einzelne Malware-Attacken. Diese sind eher Mittel zum Zweck für die Akteure dahinter. Um die Sicherheit von Infrastrukturen, Behörden und Unternehmen zu erhöhen, muss man immer auch die abstraktere Ebene und den „Faktor Mensch" hinter jeder konkreten Bedrohung bedenken.

OpenText

OpenText, The Information Company, vereinfacht, transformiert und beschleunigt die Informationsgewinnung in Unternehmen, auf der Basis von marktführenden On-Premise und Cloud-Technologien. Weitere Informationen über OpenText (NASDAQ: OTEX, TSX: OTEX) sind unter *www.opentext.de* zu finden.

Kaspersky erhält ISO 27001-Zertifizierung

Kaspersky hat am 13. Februar 2020 vom TÜV AUSTRIA die ISO/IEC 27001:2013-Zertifizierung, ein international anerkannter Standard für Informationssicherheits-Managementsysteme, erhalten. Diese bestätigt, dass die Datensicherheitssysteme des Unternehmens, einschließlich des Kaspersky Security Network, den bewährten Praktiken der Branche entsprechen.

ISO/IEC 27001 ist die weitverbreitetste Norm für Informationssicherheit, die von der International Organization for Standardization (ISO), dem weltweit größten Entwickler freiwilliger internationaler Standards, erarbeitet und veröffentlicht wurde. Sie enthält Anforderungen an die Implementierung, Überwachung, Wartung und kontinuierliche Verbesserung von Informationssicherheits-Managementsystemen (Information Security Management System, ISMS) innerhalb von Unternehmen und deren Geschäftsanforderungen. Die Konformität mit diesem international anerkannten Standard bildet die Basis von Kaspersky zur Implementierung und Verwaltung der Informationssicherheit, da er die Vollständigkeit und Genauigkeit der Sicherheitskontrollen beweist und den Kunden ein zusätzliches Maß an Sicherheit bietet.

Die Zertifizierung wurde nach einer Bewertung durch die unabhängige Zertifizierungsstelle des TÜV AUSTRIA validiert. Diese umfasste Managementsysteme zur Identifizierung bösartiger und verdächtiger Dateien unter Verwendung der Infrastruktur des Kaspersky Security Network (KSN) sowie die sichere Speicherung und den vertrauenswürdigen Zugriff auf die Dateien im Distributed File System (KLDFS) des Unternehmens. Darin inkludiert sind auch die Rechenzentren des Unternehmens in Zürich, Frankfurt, Toronto und Moskau.

„Die ISO 27001-Zertifizierung ist ein bedeutender Erfolg für Kaspersky", kommentiert Andrey Evdokimov, Chief Information Security Officer bei Kaspersky. „Sie zeigt unseren Kunden und Partnern, dass wir die Kontrolle unseres Sicherheitsmanagements als überaus hohe Priorität betrachten und erkennt unsere Herangehensweise an das Thema Informationssicherheit als nachprüfbar an. Das strenge Audit, das für die Zertifizierung durchgeführt wurde, bestätigt, dass wir uns zu höchster Datensicherheit verpflichtet haben, und stellt einen weiteren Schritt in unserem Engagement dar, die Transparenz unseres Unternehmens zu unterstreichen."

Die Zertifizierung ist im TÜV AUSTRIA-Zertifikatsverzeichnis und auf der Kaspersky-Website [2] öffentlich einsehbar. Das ISO-27001-Audit ist ein weiterer Schritt im Rahmen der im Jahr 2017 angekündigten Globalen Transparenzinitiative, die Partnern und Kunden umfassende Sicherheit darüber geben soll, dass die Produkte und Dienstleistungen des Unternehmens nicht nur den besten Schutz vor Cyber-Bedrohungen bieten, sondern auch die Kundendaten mit maximaler Sorgfalt behandelt werden. Im Jahr 2019 absolvierte das Unternehmen erfolgreich das SOC 2 Typ 1-Audit, das durch eines der vier großen globalen Wirtschaftsprüfungsgesellschaften durchgeführt wurde. Damit wurde bestätigt, dass Entwicklung und Ausspielung der AV-Datenbanken von Kaspersky durch starke Sicherheitskontrollen vor unbefugten Änderungen geschützt sind.

Weitere Informationen über die neuesten Entwicklungen innerhalb der Globalen Transparenzinitiative von Kaspersky unter *https://www.kaspersky.de/about/transparency*

TÜViT und Fraunhofer AISEC entwickeln Ansatz zur Zertifizierung von KI-Algorithmen

Maschinelle Lernverfahren und Systeme der Künstlichen Intelligenz (KI) werden bereits heute in zahlreichen IT-Infrastrukturen und vernetzten Endgeräten als zentraler Baustein zur Analyse, Prognose und Steuerung eingesetzt, gleichzeitig wird in Deutschland zunehmend die Forderung nach mehr Sicherheit beim Einsatz Künstlicher Intelligenz (KI) laut. Das zeigt eine nun veröffentlichte repräsentative Umfrage des TÜV-Verbands. Dieser zufolge wünschen sich 78% der Bevölkerung Gesetze und Vorschriften zur Regulierung von KI. 85% sind gar der Meinung, dass KI-Produkte erst auf den Markt gebracht werden sollten, wenn ihre Sicherheit von unabhängigen Stellen überprüft wurde. Das zu ermöglichen, hat sich die TÜV Informationstechnik GmbH (TÜViT) schon vor Monaten auf die Fahnen geschrieben und entwickelt sich seitdem zielstrebig zum Algorithmen-TÜV. Vor diesem Hintergrund erarbeitet TÜViT gemeinsam mit Fraunhofer AISEC aktuell Verfahren, die die Vertrauenswürdigkeit von KI-Anwendungen mess- und überprüfbar machen sollen, da diese für Unternehmen aller Branchen, aber auch für staatliche Institutionen von höchster Wichtigkeit ist.

„Da KI für Firmen viel Potential mit sich bringt und zunehmend auch in sicherheitskritischen Bereichen eingesetzt wird, möchten wir Unternehmen bei der Entwicklung von KI-Lösungen unterstützen. Daher befindet sich TÜViT gemeinsam mit dem Fraunhofer AISEC aktuell in einem Forschungsprojekt zur Prüfung Künstlicher Intelligenz", so Dirk Kretzschmar, Geschäftsführer der TÜV Informationstechnik GmbH. „Ziel ist es, ein umfangreiches Framework zu entwickeln, welches die Robustheit von KI-Anwendungen gegen mögliche Angriffe mittels speziell entwickelter Tests messbar macht."

Mithilfe des innovativen Prüfverfahrens, das in Zukunft eine valide Risikobewertung ermöglicht, werden KI-Lösungen transparenter, vergleichbarer und somit zertifizierbar. Im Fokus steht dabei der Aspekt der IT-Sicherheit und damit die Frage, wie sich die Robustheit eines KI-Algorithmus gegenüber Hackerangriffen ermitteln lässt. Auch wenn KI heute bereits in einigen Bereichen teilweise besser ist als der Mensch, können schon kleinste Manipulationen verheerende Auswirkungen haben. „Daten können so verändert werden, dass der Algorithmus ein Stoppschild plötzlich als Vorfahrtsschild erkennt", erklärt Vasilios Danos, Berater für IT-Security bei der TÜV Informationstechnik GmbH. „Für das menschliche Auge wäre diese Manipulation kaum wahrnehmbar."

Im gemeinsamen Projekt mit dem Fraunhofer AISEC entstehen Prüfverfahren, die eine quantitative Bewertung der Robustheit und Stabilität des KI-Algorithmus und dessen Einbettung in das Gesamtsystem erlauben. Mit Hilfe der in der Abteilung Cognitive Security Technologies entwickelten Verfahren lässt sich eine quantitative Risikobewertung der KI-Kernkomponenten unter Berücksichtigung der Einsatzumgebung durchführen. Ob eine KI-Anwendung verlässlich ist, wird zukünftig transparent durch eine KI-Zertifizierung sichtbar sein.

„Allein den KI-Entwicklern zu vertrauen oder gar Herstellereigenerklärungen zuzulassen, halten wir für keine belastbare Basis. Aus unserer Sicht ist es erforderlich, KI-Prüfungen in einem zertifizierten und unabhängigen Labor durchzuführen. Denn hier sind kompetentes Expertenwissen und eine entsprechende Ausstattung gefragt. Das Fraunhofer AISEC forscht bereits seit Jahren an Verfahren, um KI-Anwendungen robuster zu machen und gegen Manipulationen abzusichern und ist damit ein idealer Projektpartner", fügt Dirk Kretzschmar hinzu.

Sobald das Grundgerüst des Frameworks fertiggestellt ist, können Pilotprojekte mit Herstellern und Entwicklern von KI-Lösungen durchgeführt werden. Erste Prüfungen und Zertifizierungen sind für Mitte 2020 geplant.

Proofpoint: Die Kosten für Insider-Bedrohungen in Unternehmen um ein Drittel gestiegen

Proofpoint, Inc. (NASDAQ: PFPT), eines der führenden Next-Generation Cybersecurity- und Compliance-Unternehmen, veröffentlichte am 03. Februar 2020 seine weltweite Studie zum Thema Insider-Bedrohungen 2020. So zeigt der Bericht, dass Unternehmen im Durchschnitt jährlich 11,45 Millionen Dollar für die Beseitigung von Insider-Bedrohungen ausgaben und mehr als zwei Monate (77 Tage) benötigten, um derartige Vorfälle aufzuarbeiten. Für die Studie wurden die Kosten und Trends analysiert, die in Zusammenhang mit fahrlässigem Verhalten, kompromittierten Accounts und bös-

willigen Insider-Bedrohungen durch Angestellte, ehemalige Mitarbeiter sowie Auftragnehmer stehen.

Im Rahmen der Studie, die das Ponemon Institute im Auftrag von Proofpoint und IBM durchgeführt hat, wurden knapp 1000 IT-Sicherheitsexperten in Nordamerika, Europa, dem Nahen Osten, Afrika und dem asiatisch-pazifischen Raum befragt. Dabei hatte jedes der befragten Unternehmen mindestens einen Vorfall zu beklagen, der von Angestellten oder ehemaligen Mitarbeitern verursacht wurde. In den letzten zwei Jahren haben dabei die Häufigkeit und die Kosten von Insider-Bedrohungen in den folgenden drei Kategorien dramatisch zugenommen:

- unvorsichtiges Verhalten der Mitarbeiter/Auftragnehmer
- kriminelle Motivation der Insider
- Identitätsdiebstahl

Zu den wichtigsten Ergebnissen des diesjährigen Global Report Cost of Insider Threats 2020 gehören:

- Organisationen, die von Insider-Bedrohungen betroffen sind, geben jährlich durchschnittlich 11,45 Millionen Dollar für die Beseitigung von Schäden aus, die von Insidern verursacht wurden – das sind 31 Prozent mehr als im Jahr 2018 (8,76 Millionen Dollar).
- Mehr als 60 Prozent solcher Vorfälle waren das Ergebnis eines unvorsichtigen Mitarbeiters oder Auftragnehmers und 23 Prozent wurden von böswilligen Insidern verursacht. Bei insgesamt 14 Prozent aller Vorfälle mit Beteiligung von Insidern waren Cyberkriminelle am Diebstahl von Anmeldedaten beteiligt.
- Auch die Zahl der Vorfälle ist in nur zwei Jahren um 47 Prozent angewachsen, von 3.200 im Jahr 2018 (Ponemon) auf nunmehr 4.700.
- Je länger ein Vorfall andauert, desto teurer wird er. Vorkommnisse, bei denen es mehr als 90 Tage dauerte, um sie zu beheben, kosteten die Organisationen im Jahresdurchschnitt 13,71 Millionen Dollar. Falls die Probleme jedoch nur weniger als 30 Tage andauerten, schlugen diese mit 7,12 Millionen Dollar zu Buche. Durchschnittlich dauerte es mehr als zwei Monate (77 Tage), um einen Insider-Zwischenfall zu beseitigen.
- Je größer die Organisation, desto mehr Insider-Ereignisse gibt es. Für große Organisationen mit mehr als 75.000 Mitarbeitern beliefen sich deren Kosten im vergangenen Jahr auf durchschnittlich 17,92 Millionen Dollar. Im Gegensatz dazu gaben kleinere Organisationen mit weniger als 500 Mitarbeitern im Durchschnitt 7,68 Millionen Dollar aus.
- Am teuersten war die Behebung von durch Insider verursachten Vorfällen im Bereich der Finanzdienstleistungen. In diesem Marktsegment gaben die Unternehmen pro Vorfall mehr für die Beseitigung von Insider-Bedrohungen aus als in jeder anderen Branche: In den vergangenen zwei Jahren betrug der durchschnittliche Aufwand hier 14,3 Millionen Dollar. Bei Unternehmen aus dem Bereich Energie- und Versorgung waren dies 11,54 Millionen Dollar und 10,24 Millionen Dollar im Einzelhandel (ein Anstieg von 38 Prozent in zwei Jahren).

Weitere Informationen finden Sie unter *www.proofpoint.com/de*.

DriveLock: Wie leben Unternehmen verschiedener Größe IT-Sicherheit?

Cyberangriffe sind längst als ernstzunehmende Bedrohung im Bewusstsein deutscher Unternehmen angekommen. Doch die Intensität, mit der gegen diese Angriffe vorgegangen wird, unterscheidet sich je nach Branche und Unternehmensgröße. Das hat DriveLock, einer der international führenden Spezialisten für IT- und Datensicherheit, mit Unterstützung der techconsult in einer am 06. Februar 2020 veröffentlichten Studie ermittelt.

Die Eckdaten: Befragt wurden über 200 Unternehmen mit bis zu 1.000 Mitarbeitern aus verschiedenen Branchen: 33% aus dem Dienstleistungssektor, 27% aus der Industrie, 13% aus dem Handel, 10% aus dem öffentlichen Sektor sowie 8% aus der Finanzbranche.

Den größten Anteil mit 38% hatten dabei Unternehmen mit 50-249 Mitarbeiter, gefolgt von Unternehmen mit 250-499 (24%) und unter 50 Mitarbeitern (23%). Großunternehmen mit einer Belegschaft von 500-999 Personen machten 15% aus.

Knapp die Hälfte der Befragten waren IT-Leiter und CIOs sowie IT-Mitarbeiter, -Administratoren und -Spezialisten. Die zweite Hälfte setzte sich zusammen aus weiteren C-Level-Positionen – CISOs eingeschlossen – Compliance-Spezialisten und Sicherheits- und Datenschutzbeauftragten.

Zuständigkeiten, Stellenwert und Umsetzung

Der IT-Leiter ist in fast allen Unternehmen haupt- oder mitverantwortlich für die IT-Sicherheit (83%). In 64% der Fälle ist es der IT-Security-Leiter. 27% der Unternehmen besetzen diese Position nicht einmal. Ähnlich schwach vertreten sind Compliance- und Governance-Verantwortliche. Die Position ist bei mehr als zwei Drittel der Unternehmen nicht vorhanden. Falls doch, haben sie im Vergleich den geringsten Einfluss (40%) auf Prozesse der IT-Sicherheit.

Die Studienergebnisse zum Thema Stellenwert sind leider wenig überraschend: Je kleiner die Unternehmen, umso seltener ist IT-Sicherheit Teil der Unternehmensstrategie. 50% bzw. 42% der Unternehmen mit weniger als 50 bzw. 50-249 Mitarbeitern setzen Security-Maßnahmen proaktiv nur punktuell um, z.B. im Rahmen von Gesetzesvorgaben oder erst nach einem Sicherheitsvorfall. Selbst bei Großunternehmen mit über 500 Mitarbeitern liegt dieser Wert noch bei 32%. Die verbleibenden 68% Prozent der Unternehmen in dieser Größenordnung sehen IT-Sicherheit als einen zentralen Bestandteil ihrer Unternehmensstrategie. Ein Grund für den hohen Anteil an punktuellen Maßnahmen ist sicherlich, dass beim Großteil der Unternehmen der IT-Leiter neben seinen zahlreichen anderen Pflichten auch für Security zuständig ist. Da ist es wenig erstaunlich, dass Cybersicherheit nur dann Beachtung findet, wenn unbedingt erforderlich wie bei der DSGVO.

In Sachen Umsetzung setzen die Unternehmen größtenteils immer noch auf die Klassiker: Lösungen wie Firewall (67%), Spamfilter (63%) und Antivirus (62%) führen die Liste an. Auch das zeigt, dass Security häufig nebenbei gehandhabt wird. Viele Unternehmen setzen einfach auf diese drei Basics bei der Umsetzung ihrer IT-Sicherheit. Dahinter folgen Schulungen (57%) und Sensibilisierungskampagnen (50%) für die eigenen Mitarbeiter – noch vor Verschlüsselungstechnologien (ca. 49%).

Das Management durch externe Dienstleister ist besonders bei der kleinsten Unternehmensgröße mit 50% (Gesamt 35%) eine der wichtigsten Eigenschaften bei der Wahl von Security-Leistungen. Generell sind externe Security Provider für Unternehmen, die sich nicht selbst um ihre Sicherheitsstrategie kümmern können bzw. wollen, am sinnvollsten. Das ist besonders dann der Fall, wenn es Unternehmen an Ressourcen mangelt wie Security-Fachkräfte oder -Know-how.

Die vollständige Studie mit weiteren spannenden Erkenntnissen finden Sie hier: *https://www.drivelock.de/*

Veranstaltungskalender

4 | 2020

Veranstaltungen April und Mai		
Zeit und Ort	**Thema der Veranstaltung**	**Veranstalter**
01. – 02. April 2020 in Frankfurt / Main	IT-Grundschutz – Zusammenfassung für Manager	DresPleier GmbH Vils 8, 84149 Velden Tel.: 08742/5870894; Fax: 03222/4170655
06. – 09. April 2020 in Berlin	Ausbildung zum BSI IT-Grundschutz-Praktiker (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20 E-Mail: akademie@dgi-ag.de
07. -08. April 2020 in Dresden	Informationssicherheit – Grundlagen, Prinzipien, Methoden	DresPleier GmbH Vils 8, 84149 Velden Tel.: 08742/5870894; Fax: 03222/4170655
20. – 23. April 2020 in Berlin	IT-Sicherheitsbeauftragter (DGI)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20 E-Mail: akademie@dgi-ag.de
20. – 24. April 2020 in Frankfurt / Main	Wireshark Protokollanalyse	ExperTeach GmbH Waldstr. 94, 63128 Dietzenbach Tel.: 06074/4868-0; Fax: 06074/4868-109
20. April 2020 in Bochum	Implementierung eines zertifizierungsfähigen ISMS nach ISO/IEC 27001	isits International School of IT Security Huestr. 30, 44787 Bochum Tel.: 0234/927898-0; Fax: 0234/927898-20 E-Mail: info@is-its.org
20 – 24. April 2020 in Köln	Informationssicherheit	VdS – Bildungszentrum Pasteurstr.17 a, 50735 Köln Tel.: 0221/7766-438; Fax: 0221/7766-499 E-Mail; lehrgang@vds.de
20. – 23. April 2020 in Berlin	Ausbildung zum IT-Sicherheitsbeauftragten (ITSiBe) / Chief Information Security Officer (CISO) gemäß ISO und BSI IT-Grundschutz (DGI®)	Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG Kurfürstendamm 57, 10707 Berlin Tel.: 030/31517389-10; Fax: 030/31517389-20 E-Mail: akademie@dgi-ag.de
29. – 30. April 2020 in Bochum	Cyber Awareness – Grundlagen Sensibilisierung	isits International School of IT Security Huestr. 30, 44787 Bochum Tel.: 0234/927898-0; Fax: 0234/927898-20 E-Mail: info@is-its.org
05. – 06. Mai 2020 in Berlin	Netzwerkforensik IPv6	Cyber Akademie Kaskelstraße 41, 10317 Berlin Tel.: 030/557412-58; Fax: 030/557412-57
05. – 06. Mai 2020 in Bonn	Praxis-Darknet: Grundlagen, Einführung und Recherche	Cyber Akademie Kaskelstraße 41, 10317 Berlin Tel.: 030/557412-58; Fax: 030/557412-57
05. – 06. Mai 2020 in Berlin	Training zur IEC 62443 Security für industrielle Steuerungs- und Automatisierungssysteme	TÜV Informationstechnik GmbH Langemarckstr. 20, 45141 Essen Tel.: 0201/8999-404; Fax: 0201/8999-888 E-Mail:info@tuvit.de
07. Mai 2020 in Bonn	Einführung in Kryptowährungen – Funktionsweise, Nutzung, Nachverfolgung	Cyber Akademie Kaskelstraße 41, 10317 Berlin Tel.: 030/557412-58; Fax: 030/557412-57
11. – 15. Mai 2020 in Karlsruhe	T.I.S.P. – TeleTrusT Information Security Professional	Secorvo Security Consulting GmbH Ettlinger Straße 12-14 76137 Karlsruhe Tel.: 0721/255171-0; Fax: 0721/255171-100

DATENSCHUTZ UND DATENSICHERHEIT

DuD – Datenschutz und Datensicherheit
Recht und Sicherheit in Informationsverarbeitung und Kommunikation
Ausgabe 4/2020, 44. Jahrgang | www.dud.de

Verlag
Springer Gabler | Springer Fachmedien Wiesbaden GmbH | Abraham-Lincoln-Straße 46 | 65189 Wiesbaden
Amtsgericht Wiesbaden, HRB 9754 | USt-IdNr. DE811148419
www.springer-gabler.de

Bezugsmöglichkeiten
Jährlich erscheinen 12 Hefte.
Jahresabonnement 2020 EUR 318,78
Jahresabonnement 2020 (Firmen, Institutionen und Bibliotheken) EUR 484,-
Jahresabonnement 2020 (Studenten) EUR 98,- oder zum Vorzugspreis EUR 149,- gültig für persönliche Mitglieder der AwV (Arbeitsgemeinschaft für wirtschaftliche Verwaltung), des BvD (Berufsverband der Datenschutzbeauftragten Deutschlands e.V.), der DVD (Deutschen Vereinigung für Datenschutz e.V.), der DGRI (Deutsche Gesellschaft für Recht und Informatik), des FIfF (Forum Informatiker/Innen für Frieden und Gesellschaftliche Verantwortung e.V.), der GI (Gesellschaft für Informatik), für persönliche Mitglieder von TeleTrusT (Der IT-Sicherheitsverband Deutschlands). Der Vorzugspreis wird eingeräumt, wenn eine Bestätigung der Mitgliedschaft bzw. eine Studienbescheinigung vorgelegt wird.

Einzelheftpreis EUR 43,-

Alle Preise gelten zuzüglich Versandkosten. Alle Bezugspreise und Versandkosten unterliegen der Preisbindung.

Bezug durch den Buchhandel oder den Verlag. Abbestellungen müssen schriftlich spätestens 6 Wochen vor Ende des Bezugszeitraumes erfolgen. Im laufenden Jahrgang kann jeweils ein Sonderheft erscheinen, das nach Umfang berechnet und den Abonnenten im Erscheinungsjahr mit einem Nachlass von 25% des jeweiligen Ladenpreises geliefert wird. Bei Nichtgefallen kann das Sonderheft innerhalb einer Frist von 3 Wochen zurückgegeben werden.

Hinweise für Autoren
Bitte beachten Sie die ausführlichen Informationen unter www.dud.de. Manuskripte möglichst in maschinenlesbarer Form (Word-Datei) an den zuständigen Herausgeber (Report: Herr Reimer, Recht: Frau Mester oder Herr Buchner und Technik: Herr Fox) senden. Leserbriefe an die Herausgeber sind erwünscht, deren Publikation und eventuelle Kürzungen vorbehalten.

Geschäftsführer
Stefanie Burgmaier
Joachim Krieger
Juliane Ritt

Gesamtleitung Produktion
Ulrike Drechsler

Leiter Media Sales
Volker Hesedenz

Abonnentenverwaltung | Leserservice
Springer Customer Service Center GmbH
Haberstr. 7 | D-69126 Heidelberg
Telefon: (06221) 345-4303
Telefax: (06221) 345-4229
Montag bis Freitag, 8.00 Uhr bis 18.00 Uhr
E-Mail: springergabler-service@springer.com

Produktmanagement
Elke Janosch
Telefon: (030) 82 787-5367
Telefax: (030) 82 787-5365
E-Mail: elke.janosch@springer.com

Anzeigen
Anzeigenverkauf: Kerstin Feindler-Koch
Telefon: (0611) 7878-217
Telefax: (0611) 7878-78217
E-Mail: kerstin.feindler@springer.com

Anzeigendisposition: Petra Steffen-Munsberg
Telefon: (0611) 7878-164
Telefax: (0611) 7878-78164
E-Mail: petra.steffen-munsberg@springer.com

Es gilt die Anzeigenpreisliste vom 01.10.2018.

Produktion
Eva-Maria Krämer

Technische Redaktion
Oliver Reimer
Am Hohlstedter Weg 1a | 99441 Großschwabhausen
Telefon: (036454) 130040
Telefax: (036454) 130041
E-Mail: oliver.reimer@cmyk.one

Satz
Oliver Reimer | Großschwabhausen

Druck und Verarbeitung
Wilco | Amersfoort | Niederlande

Gedruckt auf säurefreiem und chlorarm gebleichtem Papier. | Printed in Germany

ISSN print 1614-0702

Dieser Ausgabe liegt eine Beilage vom Kunden WEKA Akademie aus Kissing, Tüv Nord aus Hamburg und dem Verlag C.H. Beck aus München bei. Wir bitten unsere Leser und Leserinnen um Beachtung.