Redaktion: Helmut Reimer

Report

BfDI in Executive Comitee der Global Privacy Assembly gewählt

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Professor Ulrich Kelber, wurde am 15. Oktober 2020 in das Leitungsgremium der internationalen Konferenz der Datenschutzbeauftragten, die Global PrivacyAssembly (GPA), gewählt. Professor Kelber freut sich über das Vertrauen seiner fast 140 internationalen Kolleginnen und Kollegen: „In der vernetzten Welt von heute müssen wir gemeinsame Lösungen finden. Durch die Wahl haben wir die Chance, auch unsere europäischen Positionen und Sichtweisen einzubringen. Ich werde mich dafür einsetzen, dass die GPA zukünftig eine noch wichtigere Stimme in der globalen Debatte um den Datenschutz wird."

Passend hierzu einigten sich die Teilnehmer der 42. Versammlung darauf, zukünftig auch außerhalb der Konferenz gemeinsame Statements zu wichtigen globalen Datenschutzthemen zu veröffentlichen. In einer weiteren Entschließung fordert die GPA datenschutzfreundliche Lösungen im Zusammenhang mit der Covid-19 Pandemie, beispielsweise bei der Kontaktnachverfolgung. Zusammen mit Hong Kong, Kolumbien und Großbritannien brachte der BfDI eine Entschließung auf den Weg, die den Einsatz von Künstlicher Intelligenz (KI) an Bedingungen knüpft. Wenn personenbezogene Daten von einem KI-System verarbeitet werden, soll dies unter anderem transparent und diskriminierungsfrei sein. In Zweifelsfällen solle eine zusätzliche Kontrolle durch Menschen erfolgen.

Professor Kelber ist der erste deutsche Datenschutzbeauftragte, der seit dem förmlichen Bestehen dem Executive Comitee angehört. Er wurde einstimmig gewählt. Die Mitglieder werden für zwei Jahre bestimmt und können einmalig wiedergewählt werden.

Weitere Informationen unter https://globalprivacyassembly.org

Die Entschließungen der 42. GPA finden Sie unter: *http://globalprivacyassembly.org/document-archive/adopted-resolutions/*

„Security by Design" – Konzept für Informationssicherheit und Datenschutz im Produktlebenszyklus

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) veröffentlichte am 25. August 2020 eine Handreichung zur Umsetzung des Konzeptes „Security by Design". Die Publikation richtet sich an Hersteller, Anbieter und Betreiber.

Die „Security by Design"-Prinzipien sind in den gesamten Produktlebenszyklus zu integrieren – von der ersten Idee bis zum Erreichen des „End-of-Life" eines Produktes. In der Umsetzungsverantwortung stehen alle am Produkt beteiligten Unternehmensbereiche, wie beispielsweise Produktmanagement, Entwicklung, Beschaffung, Fertigung, Vertrieb, Logistik, Service sowie die IT-Sicherheits- und Datenschutzverantwortlichen.

Rolf Blunk, Leiter des TeleTrusT-AK „Security by Design": „Das Konzept sieht vor, dass Sicherheitsanforderungen bereits zu Beginn des Entwicklungsprozesses systematisch ermittelt und berücksichtigt werden, um spätere Aufwände zur Behebung von Sicherheitslücken zu verhindern oder zu minimieren."

Die TeleTrusT-Publikation vermittelt ein Grundverständnis der Gestaltungsprinzipien, beschreibt modellhaft das Vorgehen und gibt Handlungsempfehlungen für Entscheider.

Hier steht die Handreichung zum Herunterladen zur Verfügung: *www.teletrust.de/publikationen/broschueren/security-by-design/*

Kaspersky-Technologie erfüllt Anforderungen an sicheren Softwareentwicklungs-Lebenszyklus

Kaspersky Industrial CyberSecurity for Networks hat auf Basis einer unabhängigen Bewertung durch den TÜV AUSTRIA am 01. Oktober 2020 die Zertifizierung gemäß der internationalen Norm IEC 62443-4-1 für einen sicheren Softwareentwicklungs-Lebenszyklus industrieller Unternehmenslösungen erhalten. Diese wird an jene Softwareprodukte vergeben, die eine Reihe von Anforderungen zum Schutz von industriellen Prozesssteuerungssystemen in modernen Produktionsanlagen erfüllen.

Die Bedürfnisse und Erwartungen des Industriesektors im Bereich Cybersicherheit sind hoch, da der reibungslose und effiziente Betrieb von Produktionslinien und Fertigungsabläufen massiv beeinträchtigt wird, wenn kritische Systeme von Cyberbedrohungen betroffen sind. Eine zuverlässige und robuste Cybersicherheitslösung ist dabei von entscheidender Bedeutung. Der Zusatz 4-1 der Norm IEC 62443 gibt Herstellern, Integratoren und Anlagenbetreibern die Gewissheit, dass die Software-Maßnahmen, die sie zur Risikominimierung in Industrieumgebungen ergreifen, in puncto Produktdesign, Qualität, Sicherheit, Implementierung und Außerbetriebnahme dem höchsten Standard entsprechen.

Erfolgreicher Audit ergibt richtlinienkonforme Prozesse

Um diese Zertifizierung zu erhalten, wurde ‚Kaspersky Industrial CyberSecurity for Networks' einem unabhängigen Audit durch den TÜV AUSTRIA unterzogen, der den gesamten Lebenszyklus des Produkts sowie den sicheren und strukturierten Ansatz bei der Softwareentwicklung überprüft hat. Die Bewertung basiert auf einer Evaluierung von mehr als vier Dutzend Metriken bezüglich des Reifegrades der Lösung. Die Kriterien umfassten den Entwurf, die richtlinienkonforme Implementierung, das Testen und die Validierung, die Beseitigung von Mängeln und die sichere Außerbetriebnahme.

„Der TÜV AUSTRIA ist eine der ersten Institutionen, die die Lücke zwischen IT- und OT-Security schließt und einen ganzheitlichen Audit-Ansatz bietet, der alle Aspekte abdeckt", kommentiert Detlev Henze, Leiter bei TÜV TRUST IT GmbH der TÜV AUSTRIA Gruppe. „IEC62443 definiert einen neuen Grad an Zuverlässigkeit für

OT-Sicherheitsprozessnetzwerke, wobei der Schwerpunkt auch auf einer qualitativ hochwertigen Softwareentwicklung liegt, die den gesamten Lebenszyklus abdeckt. Bei der Durchführung der Audits fanden wir eine hoch qualifizierte und professionelle Softwareentwicklungsumgebung vor, die den Grundstein für hochwertige Softwareprodukte legt. Die erfolgreich durchgeführten Audits zeigen, dass die Softwareentwicklungsprozesse von Kaspersky ein hohes Qualitätsniveau gewährleisten, um den verschiedenen Stufen von Risiken und Schwachstellen im Industriesektor gerecht zu werden."

Kaspersky Industrial CyberSecurity for Networks hat damit die dritte Reifegradstufe für sichere Entwicklungsprozesse erreicht und dokumentierte Prozesse demonstriert, die wiederholbar sind und konsequent befolgt werden. Die Lösung hat zudem bereits viele Kriterien der Stufe 4 erfüllt, die sich auf Optimierungsprozesse beziehen.

Weitere Informationen zur Zertifizierung und zur Lösung Kaspersky Industrial CyberSecurity for Networks sind verfügbar unter *https://ics.kaspersky.de/.*

Cybersicherheit: Industrie- und Fertigungsbranche besonders gefordert

Die gesamte Wertschöpfungskette vor Cyberattacken zu schützen zählt in der zunehmend digitalisierten Welt zu den größten Herausforderungen. Besonders der Industrie- und Fertigungsbranche fällt es schwer, Cyberrisiken in ihren Unternehmen und entlang ihrer Lieferkette zu mindern. Das ist ein zentrales Ergebnis einer am 01. Oktober 2020 veröffentlichten branchenübergreifenden Studie von TÜV Rheinland und dem Ponemon Institute zur Cybersicherheit in Unternehmen. Knapp zwei Drittel der befragten Fachleute aus der Industrie räumen Schwierigkeiten ein, während dies nur rund die Hälfte der Fachleute aus anderen Branchen bestätigt. „Unternehmen aus Industrie und Fertigung sind aufgrund des derzeitigen Digitalisierungsdrucks und dem damit resultierenden strukturellen Wandel besonders von Sicherheitsrisiken betroffen", sagt Wolfgang Kiener, Experte für Cybersicherheit bei TÜV Rheinland. „Maschinen mit einer Lebenszeit von mehreren Jahrzehnten werden digitalisiert und mit dem Internet vernetzt. Das reicht aber nicht aus. Eine ganzheitliche Cybersicherheit für unterschiedliche Systeme in komplexen Umgebungen ist absolut notwendig."

Industrielle Sicherheit gehört ins Topmanagement

Es gilt vor allem, die sogenannte „Operational Technology" (OT) zu schützen. Zur OT zählen Geräte und Systeme, die industrielle Prozesse steuern – etwa Motoren, Pumpen oder Ventile. Erfolgreiche Cyberangriffe auf diese Systeme führen zu besonders hohen Schäden. Bisher wurden zum Schutz der OT Schwachstellen oftmals nur punktuell behoben. „Ein Pflaster über eine Wunde zu kleben reicht allein nicht aus. Stattdessen sollte man sicherstellen, dass man das Verletzungsrisiko minimiert", betont Kiener. Zu diesem Zweck müsse das Thema Cybersecurity in der Topmanagement-Ebene eines Unternehmens angesiedelt sein. Viel zu häufig liege die Verantwortung jedoch in der IT-Abteilung, die keine Weisungsbefugnis für andere Unternehmenszweige wie zum Beispiel die Produktion besitzt. „Eine übergeordnete Instanz ist zwingend nötig. Nur so kann Cybersicherheit unternehmensweit mitbedacht und ganzheitlich angewendet werden", betont Kiener.

Langjährige Expertise

Seit 20 Jahren beschäftigt sich TÜV Rheinland intensiv mit den Risiken von Cyberangriffen. Die Experten beraten Unternehmen und stellen angewandte Cybersicherheitssysteme beispielsweise durch Penetrationstests auf die Probe. „Wir wissen, wie groß die Gefahr durch Cyberattacken ist, schließlich haben wir uns schon häufig – im Auftrag von Unternehmen – in äußerst sensible Maschinen und Systeme gehackt", erläutert Kiener. Eine Gefahr, der sich viele Unternehmen inzwischen zwar bewusst sind, doch fehlt es ihnen an effektiven Abwehrstrategien – das macht die Studie „Industrielle Sicherheit 2020 – eine internationale Studie zum Status quo" deutlich. Für diese befragte das unabhängige Marktforschungsunternehmen Ponemon Institute weltweit mehr als 2.200 Fachleute für Cybersicherheit aus den Branchen Automobil, Gesundheit und Pharma sowie Logistik, Verkehr, Maschinenbau und Energieversorgungsunternehmen.

Die Studie steht zum kostenlosen Download unter *www.tuv.com/industrielle-sicherheit* zur Verfügung.

Emotet in verschlüsselten Anhängen – Eine wachsende Cyberbedrohung

Die Cyberkriminellen hinter dem Banking-Trojaner Emotet unternehmen viel, um mit verschiedensten Tricks Anti-Viren-Filter zu umgehen und die Malware auf noch mehr Systemen zu verbreiten. Von Email Conversation Thread Hijacking, über Änderungen der Webshells bis hin zum Update des Emotet-Loaders, was zu einem enormen Anstieg an Downloadzahlen der Malware führte. Nun versendet Emotet erneut verschlüsselte Anhänge über seinen Malspam, um sein Botnet-Netzwerk weiter ausbauen.

Seit September 2020 beobachtet das Hornetsecurity Security Lab einen erheblichen Zuwachs an Emotet-Malspam, welcher wieder verschlüsselte Archiv-Dateien versendet. Das Passwort zur Entschlüsselung der Datei ist als Klartext im E-Mail Anschreiben enthalten. Durch die Verschlüsselung des Anhangs ist es herkömmlichen Anti-Viren-Programmen nicht möglich, das versteckte Schadprogramm zu entdecken und zu blockieren. Jedoch kann das Opfer die Datei entschlüsseln, öffnen und ausführen, wodurch die Malware schließlich nachgeladen wird.

Doch diese Methode ist nicht neu: Bereits im April 2019 entdeckten Security-Analysten erste Wellen des Emotet-Malspams mit verschlüsselten Zip-Dateien. Seitdem treten solche Spamwellen immer mal wieder verteilt über das Jahr auf und halten einige wenige Tage an. Als Operation „Zip Lock" bezeichnet die White-Hat-Group „Cryptolaemus" dieses Vorgehen der Akteure hinter Emotet. Das Team aus über 20 Security Forschern und System Administratoren hat sich als Ziel gesetzt, die Verbreitung der „gefährlichsten Malware der Welt" einzudämmen. Täglich veröffentlicht die Gruppe sämtliche Updates von Emotet auf ihrer Website und dem Twitter-Account. Damit System- und Netzwerkadministratoren die sogenannten Indicators of compromise (IOCs), dazu gehören IP-Adressen für Emotet Befehlsserver, Betreffzeilen und Datei-Hashes

von Emotet-infizierten Dateien, in ihren Security-Filtern eintragen und sich so vor möglichen Emotet-Infektionen schützen können.

Die aktuelle Malspam-Welle mit verschlüsselten Archiven sei nun bereits seit mindestens 1. September aktiv und zielte zuerst auf den japanisch-sprachigen Raum. Das Hornetsecurity Security Lab registrierte schließlich Spam-Wellen auf Spanisch, Englisch und Deutsch ab etwa dem 14. September.

Um die Chance noch weiter zu erhöhen, dass ihr Opfer die Schad-Mail beim Eintreffen im Postfach auch tatsächlich öffnet und den Anhang aktiviert, bedienen sich die Cyberkriminellen zusätzlich der „Email Conversation Thread Hijacking" Technik. Dabei werden bereits bestehende E-Mail-Konversations-Threads des Opfers verwendet, um „authentischer" zu wirken. Die Angreifer antworten dann auf bestehende Unterhaltungen, die ihr Angriffsziel in der Mailbox noch gespeichert hat.

Ein beliebter Cybercrime-Trend

Generell ist die E-Mail Angriffsmethode mit verschlüsselten Anhängen recht beliebt unter cyberkriminellen Gruppen. So entdeckten die Security-Analysten von Hornetsecurity auch in Malware-Kampagnen von GandCrab verschlüsselte Office-Dokumente und die Malware Ursnif verbreitet sich ebenfalls durch verschlüsselte Zip-Anhänge.

Wie kann ich mich davor schützen?

Die verschlüsselten Emotet-Dateien werden bis heute nicht von herkömmlichen Antivirenprogrammen entdeckt, dass beweist der Malwarescanner Dienst VirusTotal.

Auch die Technik des Email Conversation Thread Hijacking trägt zum „Erfolg" der Cyberkriminellen bei, denn für die Empfänger ist es kaum möglich, einen solchen Angriff zu erkennen, da die Schad-E-Mails von einem legitimen, aber kompromittierten Konto versendet werden.

Tiefergehende Filter und intelligente Security-Mechanismen sind jedoch in der Lage, beide dieser Angriffstechniken zu entdecken und diese vom Postfach des Empfängers fernzuhalten. Das Vorgehen der Cyberkriminellen hinter Emotet verdeutlicht, dass es auch für Unternehmen an der Zeit ist, den nächsten Schritt im Bereich der Cybersecurity zu gehen. Denn erfolgreiche Attacken treiben die Ambitionen der Hacker weiter an und bringen auch weitere Cyberkriminelle auf den Plan.

Weitere Informationen unter: *https://www.hornetsecurity.com/...*

Phishing-Mails 2.0 sind auch ohne Link gefährlich

Bisher war klar: eine E-Mail mit einem seltsamen Link – Finger weg! Aber jetzt haben die Phishing-Gangster einen neuen Trick ersonnen, um Anwender ganz ohne Links hinters Licht zu führen. Doch auch diese Betrugsattacken lassen sich mit ein bisschen Aufmerksamkeit rechtzeitig erkennen und neutralisieren.

Es ist das ewige "Spiel" zwischen Security-Spezialisten und Cybergaunern: wer ist schneller, kreativer und hat den längeren Atem. Getreu nach diesem Motto haben sich die Internetschurken wieder etwas Neues einfallen lassen: Phishing-E-Mails ohne Link.

Die meisten Phishing-E-Mails sind auf drei wesentlichen Komponenten aufgebaut:

- Eine E-Mail mit einem Link, auf den der Anwender klicken soll.
- Eine Fake-Webseite, auf der sich der Anwender einloggen soll.
- Eine weiter oder dieselbe Internetseite, welche die Login-Daten an die Gangster übermittelt

Die SophosLabs haben nun zwei außergewöhnliche Phishing-Attacken analysiert, die einen anderen Weg gehen. Bei diesen erfolgt die Aufforderung zum Login nicht über einen Link, sondern über einen HTML-Anhang. Mit diesem „Bring-Your-Own-Website"-Trick verfolgen die Cybergauner zwei Intentionen:

- In der Phishing-E-Mail befindet sich kein Link, den man im Voraus auf gefälschte oder verdächtige Domänennamen prüfen könnte.
- Die URL in der Adressleiste ist ein harmlos aussehender lokaler Dateiname ohne Website-Name oder HTTPS-Zertifikat. Auch hier ist eine Untersuchung auf Anzeichen von Betrug für den Anwender nur schwer möglich.

Mit diesem Vorgehen versuchen die Mail-Versender die Achtsamkeit der Anwender zu unterlaufen. Das wichtigste Ziel ist es, den Anwender von der vermeintlichen Ungefährlichkeit des Anhangs zu überzeugen und damit eine der schwierigsten Hürden für ihre Jagd auf Anmeldedaten zu nehmen, die in diesem Fall über die angehängte Internetseite abgezogen werden sollen. Dabei dies nicht passiert, sollten Nutzer solchen Phishing-Attacken mit den folgenden Tipps vorbeugen:

- HTM- oder HTML-Anhänge möglichst ignorieren
- Nutzung einer Zwei-Faktor-Authentifizierung
- Nutzung einer wirksamen Web-Filterung, wie beispielsweise mit dem kostenlosen Sophos Home

Und natürlich sollte beim Verdacht, einem Phishing-Angriff auf den Leim gegangen zu sein, sofort das Passwort des entsprechenden Services geändert werden. Auf Sophos Naked Security sind weitere Details zu den Phishing-E-Mails 2.0 anschaulich mit vielen Screenshots beschrieben. Zum kompletten englischen Beitrag geht es hier: *https://nakedsecurity.sophos.com/2020/10/02/serious-security-phishing-without-links-when-phishers-bring-along-their-own-webpages/*

Proofpoint: People Centric Cybersecurity – Phishing ist das häufigste Sicherheitsproblem

Proofpoint, Inc., (NASDAQ: PFPT), eines der führenden Next-Generation Cybersecurity- und Compliance-Unternehmen, veröffentlichte am 07. Oktober 2020 die Ergebnisse einer neuen Studie zum Stand der Cybersecurity in Deutschland, Österreich und der Schweiz: Die dabei gewonnenen Erkenntnisse sind alarmierend für Unternehmen aus dem deutschen Sprachraum und das über alle Organisationsgrößen und Branchen hinweg. Aus der Studie mit dem Titel „People Centric Cybersecurity" geht hervor, dass bereits 67 Prozent der befragten Unternehmen Opfer von Cyberkriminalität waren, jedes zweite davon sogar mehrfach. Oft sind die Schäden, die durch Diebstahl von Geschäftsgeheimnissen, Störungen der Betriebsabläufe oder Verlust von Stammkunden hervorgerufen werden, langfristig spürbar.

Die Anzahl von erfolglosen Angriffsversuchen Cyberkrimineller auf Unternehmen lässt sich seit langem nicht mehr beziffern. Doch trotz aller Vorsichtsmaßnahmen aufseiten der Organisationen sind die Attacken aus Sicht der Kriminellen regelmäßig von Erfolg gekrönt. Das legen die Aussagen von mehr als 200 Cybersecurity-Verantwortlichen in Deutschland, Österreich und der Schweiz nahe, die an einer Umfrage im Auftrag von Proofpoint teilgenommen ha-

ben. Dabei zeigt sich, dass Hacker in den aller seltensten Fällen die technischen Schwachstellen von Systemen ausnutzen. Viel mehr versuchen sie überwiegend E-Mails unmittelbar an einzelne Mitarbeiter zu schicken, oft mit gefälschtem Absender und frei erfundenen Inhalten. Durch diese Betrugs-E-Mails sollen die Angestellten dazu verleitet werden, sensible Daten preiszugeben oder direkt Geld auf die Konten der Kriminellen zu überweisen. So stimmten ganze 70 Prozent der befragten IT-Sicherheitsverantwortlichen aus D/A/CH zu, dass der Faktor Mensch und mangelndes Sicherheitsbewusstsein die größten Risiken für Unternehmen darstellen.

Langfristige Konsequenzen

Fallen Mitarbeiter auf die Tricks der Betrüger herein, sind die Schäden oft noch sehr lange spürbar. So hatten vier von zehn der befragten Unternehmen den Verlust sensibler Daten zu beklagen. Etwa genauso viele verzeichneten Störungen in den Betriebsabläufen.

Doch auch neben diesen direkten Auswirkungen gibt es weitere Folgen, mit denen die betroffenen Organisationen langfristig zu kämpfen haben. So hatte ein Drittel der Unternehmen Reputationsverluste im Markt zu verzeichnen, und bei jedem vierten Betroffenen verabschiedete sich ein Teil der Stammkundschaft.

Eine weitere Erkenntnis der Studie ist, dass drei von vier Unternehmen nicht optimal auf digitale Angriffe vorbereitet sind. Lediglich 24 Prozent aller Befragten konnten die Frage, ob sie auf eine Cyberattacke vorbereitet seien, vorbehaltlos bejahen. Für die Hacker besonders lohnenswerte Ziele sind dabei große Unternehmen mit mehr als 5.000 Mitarbeitern, denn von ihnen gaben lediglich 12 Prozent an, vorbereitet zu sein. Und auch der öffentliche Sektor gibt eher ein trauriges Bild ab: Während sich immerhin fast drei von vier privatwirtschaftlichen Unternehmen teilweise auf digitale Attacken vorbereitet haben (72 Prozent), konnte dies in der öffentlichen Verwaltung mit 46 Prozent noch nicht einmal jeder Zweite von sich behaupten.

Geringes Vertrauen in eigene Mitarbeiter und zu wenig Weiterbildung

„Unsere Studie zeigt, dass Cyberkriminelle sehr erfolgreich sind, Menschen in Unternehmen zu unbedachten Handlungen zu bewegen", erklärt Michael Heuer, Vice President DACH von Proofpoint. „Die Schäden, die erfolgreiche Cyberattacken nach sich ziehen, sind oft gravierend und können das Überleben einer ganzen Organisation langfristig in Frage stellen. Da sich die Angreifer fast nur noch auf das Manipulieren der Mitarbeiter konzentrieren, sollten viele Unternehmen ihre Sicherheitsstrategie dringend anpassen. Sicherheitslösungen, die sich lediglich auf technische Aspekte konzentrieren, reichen längst nicht mehr. Nur das Zusammenspiel von Mensch und Technik bringt den Organisationen nachhaltige Verbesserung der digitalen Sicherheit."

Bemerkenswert ist hierbei, dass 53 Prozent der befragten CSOs und CISOs der Meinung sind, dass ihre Mitarbeiter anfällig für Cyberangriffe seien. 77 Prozent jedoch genau hier an Schulungen sparen – in drei von vier Organisationen wird höchstens zwei Mal pro Jahr eine Cybersicherheits-Schulung durchgeführt. Auch hier bildet der öffentliche Sektor das Schlusslicht: ganze fünf von sechs Organisationen führen zu diesem Thema höchstens zwei Mal im Jahr entsprechende Trainings durch.

Phishing bleibt größtes Problem

Für die IT-Verantwortlichen bleibt in puncto Cybersicherheit Phishing das häufigste Problem. Dieser Ansicht ist zumindest jeder zweite Befragte. Auf Platz 2 liegt interessanterweise ein Bereich, der in der Vergangenheit nicht ganz so große Beachtung fand: Die Rede ist von Insider Threats. Jeder dritte (35 Prozent) sieht darin künftig ein großes Sicherheitsproblem, noch vor Ransomware mit 32 Prozent.

Und auch die COVID-19-Pandemie hat einen Einfluss hinsichtlich der Einschätzung zur gegenwärtigen Bedrohungslage von Unternehmen – allerdings in unterschiedlichem Ausmaß. Zwar beobachteten 34 Prozent der Unternehmen eine Zunahme von Phishing-Attacken seit Beginn der Pandemie, doch immerhin 29 Prozent der Befragten konnten diesen Trend nicht bestätigen.

Ferner zeigen sich massive Unterschiede zwischen den unterschiedlichen Branchen: So waren es im öffentlichen Sektor gerade einmal 15 Prozent der CIOs/CISOs, die eine Zunahme der Attacken wahrgenommen haben, wohingegen es in der Fertigungsindustrie und dem Einzelhandel mit 45 Prozentpunkten drei Mal so viele waren. Spitzenreiter im negativen Sinne war die Logistik-Branche. Mehr als 56 Prozent der Unternehmen hatten während der Pandemie einen Zuwachs an Phishing-Attacken zu verzeichnen.

Für diese Studie haben die Marktforscher von techconsult mehr als zweihundert CSOs und CISOs in Deutschland, Österreich und der Schweiz im Juli und August 2020 befragt. Diese waren in Unternehmen beschäftigt, die mindestens 250 Angestellte hatten. Berücksichtigt wurde darüber hinaus, dass diese Organisationen aus unterschiedlichen Branchen stammten wie der industriellen Fertigung, dem Einzelhandel, dem Dienstleistungssektor, der Logistik, Versorgungsunternehmen, dem Finanz- und Versicherungsbereich sowie der öffentlichen Verwaltung.

KassenSichV: TÜViT prüft erste cloud-basierte Technische Sicherheitseinrichtung für Kassen

Gemeinsame Cloud-Lösung der Bundesdruckerei-Tochter D-TRUST und der Deutschen Fiskal erhält BSI-Zertifikat nach TR-03153. TÜViT hat die cloud-basierte Technische Sicherheitseinrichtung (TSE) geprüft und durch den Zertifizierungsprozess begleitet.

Monate an Arbeit liegen hinter allen Beteiligten: Sie haben konzipiert, entwickelt, geprüft und immer wieder optimiert. Jetzt ist sie endlich abgeschlossen: Die erfolgreiche Zertifizierung nach BSI TR-03153. Erhalten hat sie die gemeinsam entwickelte cloud-basierte TSE der Bundesdruckerei-Tochter D-TRUST und der Deutschen Fiskal. Auf ihrem Weg zum BSI-Zertifikat begleitet wurden die beiden Unternehmen dabei durch die TÜV Informationstechnik GmbH (TÜViT), die die Cloud-Lösung auf die Anforderungen der TR-03153 hin geprüft und einen entsprechenden Bericht zur Vorlage beim BSI erstellt hat. Nach eingehender Prüfung hat die Behörde das TR-Zertifikat nun – und damit pünktlich zum Ende der Nichtbeanstandungsfrist – erteilt.

Die erfolgreiche Zertifizierung belegt, dass die TSE-Cloud die Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie die Forderungen der Kassensicherungsverordnung (KassenSichV) angemessen erfüllt. „Wir freuen uns und sind stolz, dass unsere komplett neue Lösung auf modernster technologischer Basis als erste zertifizierte TSE-Cloud an den Markt geht. Als Ergänzung zur Hardware-Lösung ermöglichen wir so eine von vielen Kunden gewünschte, technologieoffene Umsetzung des Kas-

sengesetzes", sagt Dr. Kim Nguyen, Geschäftsführer von D-TRUST GmbH. Bei der Fiskal Cloud handelt es sich um eine TSE-Lösung für auf Windows und Linux basierende Systeme, die es unabhängig vom Ort des Kassensystems ermöglicht, alle Kasseneingaben mit Beginn des Aufzeichnungsvorgangs zu protokollieren und elektronisch zu signieren. Damit einher geht gleichzeitig ein geringerer Installations- und Wartungsaufwand, da Einzelumrüstungen vermieden werden und notwendige Anpassungen nur einmal zentral in der Cloud umgesetzt werden müssen.

Freude über die abgeschlossene Zertifizierung herrscht auch auf Seiten TÜViT's. „Da das Produkt die erste cloudbasierte TSE-Lösung ist, die sich bei uns im Zertifizierungsprozess befunden hat, war das Projekt auch für uns zunächst Neuland. Umso zufriedener sind wir, dass alle Tests erfolgreich durchgeführt und der Zeitplan bis zum 30. September eingehalten werden konnte", so Dirk Kretzschmar, Geschäftsführer der TÜV Informationstechnik GmbH.

Wurde durch die KassenSichV zunächst gefordert, dass alle Aufzeichnungssysteme ab Januar 2020 über eine zertifizierte TSE verfügen, gab das Bundesministerium für Finanzen (BMF) Unternehmen in Form der Nichtbeanstandungsregelung für die Umsetzung noch einmal Zeit bis Ende September 2020. Angesichts der aktuellen Corona-Situation gewähren alle Bundesländer bis auf Bremen unter bestimmten Bedingungen einen weiteren Aufschub bis zum 31. März 2021. TÜViT bietet Herstellern von Kassensystemen die gesetzlich geforderte Prüfung nach TR-03153 auch weiterhin an und begleitet sie entlang des gesamten Zertifizierungsprozesses.

BMI: 9-Punkte-Plan für ein digitales Deutschland

Nach zwei Monaten im Amt benennt Bundes-CIO und Staatssekretär im BMI Dr. Markus Richter neun Schwerpunkte, mit denen die Digitalisierung in Deutschland vorangebracht werden soll.

Der Plan bringt die drei zentralen Säulen der Digitalisierung im Bundesministerium des Innern, für Bau und Heimat zusammen: Digitale Gesellschaft, Digitale Verwaltung sowie Cyber- und Informationssicherheit.

Richter sieht das BMI als Treiber der Digitalisierung von Gesellschaft und Verwaltung. Dabei sind für ihn die Anforderungen Datenschutz und Transparenz kein Widerspruch, sondern bilden die einheitliche Grundlage für ein europäisches, wertebasiertes Digitalmodell, das sich von anderen Modellen in der Welt unterscheidet.

„Mir ist die Einbindung der Bürgerinnen und Bürger besonders wichtig. Denn nur, wenn sie den Prozessen vertrauen, wird die Digitalisierung erfolgreich sein können," sagt Dr. Markus Richter. „Meine Schwerpunkte werde ich deshalb im Dialog mit Bevölkerung und Unternehmen umsetzen."

Verwaltung beschleunigt digitalisieren

Wesentliche Ziele des 9-Punkte-Papiers sind die Beschleunigung der Verwaltungsdigitalisierung und die Einführung von eGovermentdiensten in Deutschland. So soll die Akzeptanz des Onlineausweises erhöht, digitale Leistungen schneller verfügbar sowie die Kommunikation mit den Behörden zugänglicher werden.

Die Nutzung und Bereitstellung von Daten soll mit einer eigenen Open-Data-Strategie vorangebracht werden. Bis Jahresende soll zudem ein Bundesportal zur besseren Auffindbarkeit von Leistungen und ein einheitliches Nutzerkonto für Unternehmen verfügbar sein. Die Kompetenzen der Verwaltungsmitarbeitenden werden mit Fortbildungsprogrammen an einer neuen Digitalakademie gestärkt, eine eigene eGovernment-Einheit widmet sich digitalen Innovationen in der Bundesverwaltung.

Cyber- und Informationssicherheit stärken

Im Bereich Cyber- und Informationssicherheit möchte Richter die Cyber-Sicherheitsstrategie aus dem Jahr 2016 evaluieren und fortschreiben. Strategisch weiterentwickeln möchte er auch die Netzinfrastrukturen der Öffentlichen Verwaltung mit einer „Netzinfrastruktur 2030" und einer „Digitalfunkstrategie 2030". Dabei soll die Rolle des Bundes insgesamt sowie des Bundesamtes für Sicherheit in der Informationstechnik gestärkt werden. Die zunehmende Vernetzung und Digitalisierung aller Lebensbereiche schaffen jedoch auch neues Gefahrenpotential. Dem möchte Richter durch eine Ausweitung des Cyber-Strafrechts auf nationaler und europäischer Ebene begegnen.

Weiteres Ziel ist, die digitale Souveränität des Staates auszubauen und Abhängigkeiten von einzelnen großen Herstellern zu reduzieren. Neue Technologien wie Künstliche Intelligenz sollen datenschutzkonform für die Verwaltung erschlossen werden.

Der 9-Punkte-Plan ist ein Beitrag, die Verwaltung für zukünftige Krisen noch besser aufzustellen. Seine Umsetzung wird mit konkreten Meilensteinen hinterlegt und in einem eigenen Controlling nachgehalten.

Dr. Markus Richter ist seit 1. Mai Beauftragter der Bundesregierung für Informationstechnik. Zuvor hat er als Vizepräsident des BAMF, die Digitalisierung im Asylwesen maßgeblich vorangebracht.

BSI-Lagebericht 2020: Corona verschärft Cyber-Gefährdungslage

Die Corona-Pandemie hat großen Einfluss auf die Cyber-Sicherheitslage in Deutschland. Corona hat für einen Digitalisierungsschub in Deutschland gesorgt, den es nachhaltig zu gestalten, aber auch abzusichern gilt. Diese und weitere Erkenntnisse zur aktuellen Gefährdungslage hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im neuen „Bericht zur Lage der IT-Sicherheit in Deutschland 2020" zusammengestellt, den Bundesinnenminister Horst Seehofer und BSI-Präsident Arne Schönbohm am 20. Oktober 2020 in Berlin vorgestellt haben.

Im Zuge der Corona-Pandemie arbeiten viele Menschen im Homeoffice. Bring-your-own-Device wird vielerorts als Mittel zur Arbeitsfähigkeit akzeptiert, viele Videokonferenzen wurden kurzfristig eingerichtet und Unterricht wird als Home-Schooling mit Laptop und Webcam abgehalten. Viele dieser Maßnahmen sind spontan umgesetzt worden. IT- und Datensicherheit spielte dabei oft eine untergeordnete Rolle.

„In der akuten Situation habe ich durchaus Verständnis dafür. Jetzt aber, nachdem sich vieles eingespielt hat, gilt es, dieses ‚neue Normal' nachhaltig und sicher zu gestalten. Tun wir dies nicht, dann werden wir die Folgen in einigen Wochen oder Monaten spüren. Wenn wir weiterhin von der Digitalisierung profitieren wollen, dann dürfen wir es Angreifern nicht zu leicht machen. Der neue Lagebericht des BSI macht aber auch deutlich, dass wir die Cyber-Sicherheit in Deutschland ein gutes Stück vorangebracht haben.

Als Cyber-Sicherheitsbehörde des Bundes übernimmt das BSI Verantwortung, indem wir uns mit den Risiken der Digitalisierung auseinandersetzen und aufzeigen, wie wir diesen wirksam begegnen können", erklärt BSI-Präsident Arne Schönbohm.

Die aktuelle Gefährdungslage ist weiterhin geprägt von Cyber-Angriffen mit Schadsoftware, die in immer neuen Varianten und mit teils ausgefeilten Methoden eingesetzt wird. Die Zahl der Schadprogramme übersteigt inzwischen die Milliardengrenze. Allein im Berichtszeitraum sind 117,4 Millionen neue Varianten hinzugekommen, somit etwa 320.000 neue Schadprogramme pro Tag. Weiterhin dominant ist die Schadsoftware Emotet, die das BSI schon vor rund zwei Jahren als gefährlichste Schadsoftware der Welt bezeichnet hatte. Sie bietet Angreifern zahlreiche fortschrittliche Angriffsmöglichkeiten. Daten werden immer öfter nicht nur verschlüsselt, sondern von Cyber-Kriminellen kopiert und ausgeleitet. Die Angreifer drohen zusätzlich damit, die Daten an Interessenten zu verkaufen oder zu veröffentlichen. Damit erhöhen die Angreifer den Druck auf das Opfer, der Lösegeldforderung nachzukommen.

Von Cyber-Angriffen betroffen sind Unternehmen und Institutionen aller Größen und Branchen. So wurden Automobilhersteller und ihre Zulieferer angegriffen, ebenso wie Flughäfen und Fluggesellschaften. Auch kleine und mittelständische Unternehmen, die sich durch Alleinstellungsmerkmale wie zum Beispiel die Produktion spezieller Komponenten im Maschinenbau auszeichnen, wurden Opfer von Cyber-Angriffen. Ebenso waren kommunale Verwaltungen, Krankenhäuser und Hochschulen von Ransomware-Angriffen betroffen.

Bemerkenswert ist die Bedrohung durch Daten-Leaks, das heißt den Diebstahl oder die unbeabsichtigte Offenlegung personenbezogener Datensätze, zum Beispiel Kundendaten oder Patientendaten. So waren in einem Fall allein in Deutschland im Zeitraum von Juli bis September 2019 etwa 15.000 Patientendatensätze mit mehreren Millionen medizinischen Bildern öffentlich ohne Passwortschutz zugänglich. Die Informationen lagen auf sogenannten PACS-Servern (Picture Archiving and Communication Systems), die im Gesundheitswesen zur Bildarchivierung genutzt werden. Das BSI hat sowohl die betroffenen medizinischen Einrichtungen in Deutschland als auch 46 internationale Partner informiert.

Weitere Informationen und Beispiele sind im „Bericht zur Lage der IT-Sicherheit in Deutschland 2020" zusammengefasst. Der Lagebericht des BSI gibt einen Überblick über die Entwicklung der Bedrohungslage im Cyber-Raum vom 1. Juni 2019 bis zum 31. Mai 2020 und über die Aktivitäten und Gegenmaßnahmen des BSI.

Cyberfibel: Nachschlagewerk für digitale Aufklärung

Anlässlich des 3. Roundtables des Bundesministeriums des Innern, für Bau und Heimat und des Bundesministeriums der Justiz und für Verbraucherschutz zur IT-Sicherheit von Verbraucherinnen und Verbrauchern am 09. Oktober 2020 haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Deutschland sicher im Netz e.V. (DsiN) heute die Cyberfibel vorgestellt. Das umfangreiche Nachschlagewerk richtet sich an Wissensvermittler und Bildungseinrichtungen. Diesen steht nun erstmalig ein Gesamtangebot zur Verfügung, das auf über 200 Seiten auf aktuelle Fragestellungen im digitalen Alltag mit konkreten Erklärungen, Hintergründen, Übungen, Handlungsempfehlungen und weiterführenden Links eingeht. Durch regelmäßige Erweiterungen werden auch künftige Entwicklungen und veränderte Sicherheitsanforderungen berücksichtigt. Die Cyberfibel ist als gedrucktes Handbuch sowie online verfügbar.

„Genauso wie wir in der Schule mit der Fibel lesen lernen, müssen wir uns auch mit den Regeln des digitalen Raums befassen. Unser Ziel im Rahmen des Digitalen Verbraucherschutzes ist es, durch Informationsangebote, technische Anforderungen und Standards Rahmenbedingungen zu schaffen, um ein sicheres und selbstbestimmtes Handeln von Verbraucherinnen und Verbrauchern in der digitalen Welt zu ermöglichen. Mit der Cyberfibel geben wir unseren Partnern in der Wissensvermittlung ein praxisorientiertes, stets aktuelles Handwerkszeug an die Hand, das sie in ihrer täglichen Arbeit mit den Bürgerinnen und Bürgern sofort einsetzen können", erklärt BSI-Präsident Arne Schönbohm.

Staatssekretär und CIO des Bundes Dr. Markus Richter erklärt: „Wir alle nutzen täglich eine Vielzahl digitaler Angebote, die uns das Leben erleichtern. Viele Verbraucherinnen und Verbraucher wünschen sich dabei mehr Anleitung und Hilfestellung, damit sie digitale Dienste und Geräte sicher einsetzen können. Ziel des Bundesinnenministeriums ist es, Menschen in jeder Lebenslage zur Teilhabe an der Digitalisierung zu befähigen. Mit der Cyberfibel schaffen BSI und DsiN dafür eine wichtige Orientierung in der Aufklärungsarbeit."

„Wir verstehen die Cyberfibel als lebendiges Werk, das auf neue Anforderungen im digitalen Alltag eingeht. Damit schaffen wir die Orientierungshilfe, welche dringend erforderlich ist, um digitale Verbraucheraufklärung auf einem einheitlichen Niveau zu entwickeln", so DsiN-Geschäftsführer Dr. Michael Littger.

Verbraucherschutzstaatssekretär Prof. Dr. Christian Kastrop erklärt: „Die Cyberfibel ist ein wichtiges Instrument für die digitale Verbraucheraufklärung. Unser Ziel ist es, dass viele Menschen von den Inhalten profitieren, indem sie die darin enthaltenen Informationen für einen sicheren digitalen Umgang in Schule, Beruf und Privatleben nutzen."

Entstanden ist die Cyberfibel auf Initiative des Deutschland Dialogs für digitale Aufklärung, dem Akteure aus der Wirtschaft, Zivilgesellschaft und Verwaltung angehören. Die Cyberfibel steht ab sofort als Onlineversion und als gedrucktes Werk zur Verfügung (*https://www.cyberfibel.de*). Die Fibel kann online über das Bestellformular angefordert werden. Pro Besteller kann ein gedrucktes Exemplar kostenfrei bezogen werden.

UNECE-Regularien für Automotive Cybersecurity verabschiedet

Das UNECE World Forum for Harmonization of Vehicle Regulations hat am 24. Juni 2020 die lang erwarteten neuen UN-Regelwerke zu Cybersicherheit und Software-Updates von vernetzten Fahrzeugen verabschiedet. Neben den 54 Vertragsparteien, darunter Deutschland und die Staaten der EU, werden auch Südkorea und Japan das Abkommen übernehmen. Inkrafttreten werden die UN-ECE-Regularien zum Januar 2021 und ab Sommer 2022 in der EU verbindlich sein.

Die Richtlinien der Vereinten Nationen legen für die Automobilhersteller klare leistungs- und Audit-Anforderungen für IT-Sicherheit und Software-Updates von Fahrzeugen fest. Sie sind die ers-

ten international harmonisierten und verbindlichen Normen in diesem Bereich überhaupt. Die UNECE-Regularien fordern dabei konkrete Maßnahmen vier Bereichen:

- Management der Cyberrisiken für Fahrzeuge
- Security-by-Design bei der Fahrzeugentwicklung, um Risiken entlang der Wertschöpfungskette zu mindern;
- Angriffserkennung und -abwehr für die gesamte Fahrzeugflotte;
- Bereitstellung sicherer Software-Updates und Einführung einer Rechtsgrundlage für Over-the-Air-Updates

Die Vorschriften gelten für PKWs, Kleintransporter, LKWs und Busse. In der Europäischen Union wird die neue Verordnung ab Juli 2022 für alle neuen Fahrzeugtypen und ab Juli 2024 für alle ab diesem Zeitpunkt hergestellten Neufahrzeuge verpflichtend. Auf die EU, Südkorea und Japan, die sich gemeinsam zu dem neuen Abkommen bekennen, entfällt rund ein Drittel der weltweiten Automobil-Produktion. Darüber hinaus gelten die neuen Cybersecurity-Anforderungen für alle Hersteller, die Fahrzeuge in diesen Ländern verkaufen möchten.

ESCRYPT verfolgt die Entwicklung der UN-Regulierung und weiterer Standards im Bereich der Automotive Security seit langem. In Zusammenarbeit mit der Unternehmungsberatung KPMG unterstützt ESCRYPT OEMs und Zulieferer weltweit bei Aufbau und Implementierung konformer Cybersecurity-Management-Systeme. Zudem bietet ESCRYPT Sicherheitsanalysen sowie Security Testing Services und professionelle Beratung für ein automotive-spezifisches Security-Design. Und stellt alle Elemente für ein Vehicle Security-Monitoring von Fahrzeugflotten im Feld bereit – von Komponenten für die Angriffserkennung im Fahrzeug (CycurIDS) und im Backend (CycurGUARD) bis hin zum Vehicle Security Operation Center (V-SOC).

Das UNECE-Abkommen im Wortlaut finden Sie hier: *https://security.cybellum.com/wp29*

Rezensionen

Bücher

Ludwig Gramlich

Jotzo, Florian: Der Schutz personenbezogener Daten in der Cloud. Nomos. Baden-Baden. 2 Aufl. 2020. 214 S. ISBN 978-3-8487-3616-4. € 58.-

Es ist eher ungewöhnlich, wenn eine Dissertation nach fast 10 Jahren in einer weithin, wenn nicht gar völlig überarbeiteten Fassung in einer zweiten Auflage erscheint und dabei die Gelegenheit nutzt, an der einen oder anderen Stelle für die frühere Rechtslage auf die ursprüngliche Version zu verweisen. Die konkrete Thematik von Cloud Computing aus juristischer (heute vor allem EU-rechtlicher) Sicht ist allerdings allemal eine erneute Befassung wert, zumal hier die Entwicklung gewiss nicht abgeschlossen ist. Jotzo hält insoweit im Vorwort fest (S. 5), in den weltweit vernetzten Strukturen der Cloud verlören einzelne Staaten mehr und mehr Einfluss, so dass es „in ihrem ureigensten Interesse" liege, sich unter dem Dach der EU (bzw. des EWR und des Europarats) „auf gemeinsame Werte zu verständigen, um diese im digitalen Raum zu behaupten". Angestrebt werde daher für „alle in Unternehmen, Gesellschaft und Wirtschaft" eine „aktuelle und prägnante Zusammenschau zum Thema Cloud und Datenschutz" (mit Stand Ende 2019).

Der wissenschaftliche Anspruch zeigt sich bereits in vorangestellten ausführlichen Literatur- und Dokumentenverzeichnissen und einem mehr als 1200 Fußnoten umfassenden Quellenapparat, ferner in durchweg zielführenden Querverweisen im Fließtext. Leider fällt insoweit das Stichwortverzeichnis etwas ab, wo der Leser etwa Compliance, CRM , Kohäsionsverfahren oder Europäischer Datenschutzausschuss vergeblich sucht bzw. zuweilen nicht alle einschlägigen Randnummern genannt werden (wie bei Housing oder Joint Controller Agreement).

In sechs Kapiteln, das letzte ein knapper Ausblick auf Chancen und Herausforderungen, bietet Jotzo eine teils sehr tief untergliederte, flüssig geschriebene Analyse, beginnend mit „Grundlagen" und mündend (vom Umfang her am ausführlichsten) in Aspekten der „grenzüberschreitenden Cloud". Dass die Einleitung kein eigenes Kapitel bildet, sondern vor „Grundsätzen des Datenschutzes" (auf Verfassungs- und Verordnungsebene) zu Beginn der „Grundlagen" (Kap. 1) platziert ist, während ein zweites allgemeines Kapitel vom „sachlich anwendbaren Datenschutzrecht" handelt, also ebenfalls noch „Grundlagen"-Charakter hat, sollte nicht weiter irritieren; inhaltlich ist die Ab- und Eingrenzung des Geltungsbereichs der DSGVO überaus differenziert und rundum überzeugend. Beim Hauptthema werden dann zunächst (allgemein) „Verantwortlichkeit" und „Datenverarbeitung" in der Cloud diskutiert, bevor der Blick über die nationalen bzw. EU-Grenzen hinaus geht und die spezifische Drittlandsproblematik erörtert, d.h. die verschiedenen Optionen der Art. 44 ff. DSGVO erläutert und bewertet. Zusammenfassungen finden sich am Ende der Kap. 1 und 3, jedoch nicht zu den Ergebnissen insgesamt in Kap. 6, wo vielmehr (wissenschaftskonform) ein echter „Ausblick" in Form neuer, offener Fragen geboten wird.

Schwerpunkt der Analyse liegen eindeutig bei der Klärung des Verantwortlichen vor allem im Kontext der hier zumeist vorliegenden, weiterhin privilegierten Auftragsverarbeitung (i.S.v. Art. 4 Nr, 8 und 28 DSGVO), wobei präzise gegenüber gemeinsamer Verantwortlichkeit (Art. 26) abgegrenzt und auf den Wegfall von Funktionsübertragung hingewiesen wird. Personell wird in der Regel der Cloud-Nutzer als Verantwortlicher (Art. 4 Nr. 7) eingeordnet, werden jedoch davon diverse Fälle der Verantwortlichkeit (auch) des Cloud-Diensteanbieters (Provider) unterschieden. Die Rechtsbeziehungen zwischen Nutzer und Provider (Auftraggeber und -nehmer) werden im Rahmen der „Verarbeitungs"-Arten und Formen näher untersucht; hier behandelt Jotzo auch (beim Vertragsinhalt) Aspekte der Rechtswahl und des Gerichtsstands, an die dann später bei der grenzüberschreitenden Cloud angeknüpft wird. Obwohl innerhalb des Auftragsverhältnisses Art. 6 DSGVO nicht eingreift, werden (als Option für externe Cloud-Anbieter) geeignete Tatbestände des Art. 6 (Abs. 1) einschließlich der Einwilligung beleuchtet und wird dabei auf die Bedeutung der Form (Dokumentation) für die Praxis hingewiesen. Überaus differenziert wird schließlich auch Art. 3 mit den dort normierten Anknüpfungsmöglichkeiten ausgebreitet und wird plausibel die Verbindung der zentralen Begriffe „Niederlassung" und „Dienstleistung" mit EU-Grundfreiheiten verdeutlicht. Die diversen Gestaltungen der Art. 45 – 49