secorvo
security consulting

Secorvo Security News

Juni 2020

Friendly Fire

Es ist nicht lange her, da galten Phishing-Angriffe als IT-Dilettanten-Test: Wer auf die holprigen, in schlechtem Englisch verfassten Aufforderungen hereinfiel und PIN und TAN für sein Konto preisgab, der konnte sich der Schadenfreude seiner Umgebung sicher sein. Die von solchen Angriffen verursachten Schäden blieben daher überschaubar, auch, weil die deutschen Banken technisch gegensteuerten: 2016 summierten sie sich auf gerade einmal 8,7 Mio. Euro.

Aber die Phisher lernten schnell, dass mit „digitalem Social Engineering" auch ganz andere Summen abgerufen werden können: Ob CEO Fraud, Verschlüsselungs-Trojaner oder Credential Phishing – alle diese Angriffsformen basieren im Kern darauf, den Empfänger mit einer halbwegs plausiblen Geschichte zu einer Schaden verursachenden Reaktion zu verleiten. Entscheidender Auslöser ist am Ende ein Klick – auf einen Link, einen Login-Knopf oder eine Online-Überweisung.

Zwar gibt es probate Mittel, um die Authentizität einer E-Mail oder eines Anrufs zu überprüfen, auf die auch ausgefuchste Angreifer keinen Einfluss haben: die interne Rückfrage, die Prüfung der Rufnummer oder E-Mail-Adresse, das Vier-Augen-Prinzip. Eine solche Aufdeckung digitaler „Enkel-Tricks" fordert jedoch Aufmerksamkeit und gesundes Misstrauen von den IT-Nutzern. Leider sind wir seit Jahren (SSN 01/2012) dabei, ihnen gerade dies abzugewöhnen.

E-Mail-Clients, die nur den vom Absender wählbaren Sendernamen statt der E-Mail-Adresse anzeigen, Online-Anbieter, die für den Rechnungsversand oder das User-Management beliebige Second-Level-Domains nutzen und Marketing-Abteilungen, die Klickraten durch HTML-formatierte E-Mails mit verdeckten Links in die Höhe zu treiben versuchen: All dies stumpft Aufmerksamkeit und Misstrauen ab. Schutz vor Täuschungsangriffen werden wir daher nicht allein durch Mitarbeiter-Sensibilisierung erreichen – auch Hersteller, Marketingabteilungen und die interne Kommunikation müssen ihren Teil der Verantwortung erkennen.

Inhalt

secorvo
security consulting

Security News

IT-Sicherheit 2.0

Mitte Mai wurde ein Referentenentwurf des Innenministeriums für das „IT-Sicherheitsgesetz 2.0“ mit Stand vom 07.05.2020 öffentlich. Zwar kann sich bis zur Gesetzesverabschiedung noch sehr viel ändern, doch verdient der Entwurf aufgrund seiner zahlreichen Neuerungen Aufmerksamkeit. So erhält das BSI neue Aufgaben, u. a. die Förderung des Verbraucherschutzes und die Entwicklung eines „Stands der Technik“ bzgl. der sicherheitstechnischen Anforderungen an IT-Produkte. Es soll zur allgemeinen Meldestelle für Sicherheitsrisiken in der Informationstechnik werden und selbst aktiv nach Sicherheitslücken von öffentlich erreichbaren IT-Systemen suchen dürfen, auch mittels simulierter Angriffe.

Den Betreibern kritischer Infrastrukturen auferlegte Pflichten werden ausgeweitet auf „Unternehmen von besonderem öffentlichen Interesse“, die durch Rechtsverordnung noch genauer zu bestimmen sind. Im Telemediengesetz (TMG) soll u. a. eine Anzeigepflicht bei Angriffen und Datenverlusten gegenüber dem Bundeskriminalamt ergänzt werden. Ein interessantes Detail ist auch die Verlängerung der Speicherdauer für Protokolldaten der Systeme des Bundes auf bis zu 18 Monate. Und nicht zuletzt werden die Sanktionen bei Verstößen auf DSGVO-Niveau angehoben.

Die Rolle des BSI wird durch den Gesetzesentwurf deutlich erweitert. Der Entwurf enthält zahlreiche Regelungen, die erhebliche Auswirkungen auf IT-Vorhaben zahlreicher Unternehmen haben werden. Die Umsetzungsfristen, soweit vorgesehen, liegen bei nur einem Jahr – ein wichtiger Grund, das Gesetzgebungsverfahren aufmerksam zu verfolgen.

Cookies - nur mit Einwilligung

Am 28.05.2020 hat der Bundesgerichtshof nach der Planet49-Entscheidung des EuGH (SSN 10/2019) nun auch ein Urteil in Sachen Cookies gefällt. Das Ergebnis ist wenig überraschend: Das Setzen von Cookies ist nur zulässig, wenn der Betroffene zuvor eingewilligt hat. Die Auffassung, dass hiervon technisch erforderliche Cookies nicht betroffen sind, teilt der BGH mit dem EuGH. Am meisten Aufsehen erregt der BGH mit seiner Auslegung des § 15 Abs. 3 Satz 1 TMG: Obwohl darin dem Wortlaut nach von einem Widerspruch die Rede ist, hat nach Überzeugung des BGH auch hier eine Einwilligung vorzuliegen.

Damit steht unzweifelhaft fest: Möchte ein Webseitenbetreiber neben technisch notwendigen Cookies und ähnlichen Technologien auch solche einsetzen, die z. B. dem Marketing dienen, benötigt er die Einwilligung des Seitenbesuchers. Klarheit darüber, wie solche Einwilligungen in der Praxis auszusehen haben, gibt es jedoch weiter nicht.

Ungewolltes Phishing-Training

Am 02.04.2020 sperrte Linksys die Konten aller „Smart-Wi-Fi“-Nutzer, nachdem bekannt geworden war, dass Angreifer über so genannte Credential-Stuffing-Attacken die Kontrolle über eine Vielzahl von Benutzerkonten erlangt hatten. Dazu probieren Angreifer aus früheren Leaks bekannte Benutzernamen und Passwörter in anderen Anwendungen aus.

Die – an sich begrüßenswerte – proaktive E-Mail von Linksys, in der die Kunden zur Rücksetzung des Passworts aufgefordert wurden, wurde jedoch nicht von einer bekannten Linksys-Domäne, sondern von subscribermanagement@linksys-email.com verschickt – typisches Merkmal einer Phishing-E-Mail. Ein vermeidbarer sicherheitskritischer Fehler: Misstrauische Nutzer werden nicht auf diese E-Mail reagiert haben, andere wurden verunsichert und einige werden wieder einmal gelernt haben, dass es doch nicht weh tut, auf zweifelhafte E-Mail-Links zu klicken.

Kein Einzelfall, wie unsere Praxiserfahrung zeigt. E-Mails mit anhängenden Bestellungen im PDF-Format ohne Begleittext, Faxe mit anderer Ortsvorwahl als die des Absenders, kryptische Servernamen und Aufforderungen, ein Benutzerkonto zu aktivieren, die von unternehmensfremden Domains verschickt werden. Vermeintliche Kleinigkeiten, die mittelfristig jedoch große Schäden verursachen können. Denn der nächste Phishing-Angriff kommt bestimmt.

Aus für Google Analytics

Die Datenschutzkonferenz hat am 12.05.2020 ihre Hinweise zum Einsatz von Google Analytics aktualisiert und die Orientierungshilfe für Anbieter von Telemedien ergänzt. In der ausdrücklich nicht abschließenden Beurteilung werden der Widerrufs-Button von Google und die Einordnung als Auftragsverarbeitung „beerdigt“. Zudem wird klargestellt, dass Google unabhängig von anonymize_IP regelmäßig mit personenbezogenen Daten arbeitet. Die Datenschutzkonferenz betrachtet die Nutzung von Analytics daher als Fall der gemeinsamen Verantwortung (Art. 26 DSGVO).

Die Nutzung von Analytics könne in der Regel nicht aus einem berechtigten Interesse abgeleitet werden, sodass eine Einwilligung der Nutzer erforderlich ist. Die Information der Betroffenen muss beinhalten, dass Google die gesammelten Daten zu „beliebigen eigenen Zwecken“ verwendet, die Daten unter Zugriff staatlicher Stellen in den USA verarbeitet und darlegen, welche Zwecke damit von Google verfolgt werden. Dazu wird auf die Leitlinien für Transparenz des EDSA vom 11.04.2018 verwiesen.

Keine dieser Anforderungen erfüllt Analytics derzeit: Es gibt kein Vertragsangebot von Google zur gemeinsamen Verantwortung, und auch technisch genügt Analytics den Anforderungen der DSK nicht. Eine informierte Einwilligung kann auch der Seitenanbieter nicht beisteuern. In aller Klarheit und Kürze: Die Nutzung von Google Analytics ist in Europa derzeit nicht rechtskonform möglich.

Thunderspy

Intels Thunderbolt-Technologie setzt sich immer weiter durch; viele Notebooks bringen bereits entsprechende Ports mit. Technisch werden dabei der DisplayPort für die Bildübertragung und PCI Express (PCIe) für eine performante Datenübertragung kombiniert. Zurzeit wird Version Thunderbolt 3 verbreitet, die die Funktionen von USB 3.1 umfasst, also den Anschluss von USB-Geräten und Ladefunktionen bietet. So eignet es sich ausgezeichnet als Docking-Port. Da PCIe auf der Basis von Direct Memory Access (DMA) arbeitet, kann darüber auf den Hauptspeicher des Computers zugegriffen werden. Um das unberechtigte Auslesen sensibler Daten und Manipulationen des Systems zu verhindern, haben Hersteller DMA Remapping und Thunderbolt Security entwickelt; darüber kann man einzelne Geräte (z. B. Docks) für PCIe autorisieren.

Nach unserer Erfahrung wird Thunderbolt Security in vielen Unternehmen jedoch deaktiviert, weil der Verwaltungsaufwand hoch ist. Der Sicherheitsforscher Björn Ruytenberg hat am 17.04.2020 in einem Paper mehrere Schwachstellen des Protokolls veröffentlicht, die es erlauben, die Sicherheitsfunktionen zu umgehen. Nach Einschätzung des Autors lassen sich die Schwachstellen kaum in Software beheben. Wer den Thunderbolt Port nutzt, sollte daher auf die Vertrauenswürdigkeit des Geräts achten.

DSGVO-konforme Auskünfte

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, hat aufgrund zahlreicher Beschwerden die Berechnungsmethoden von Wirtschaftsauskunfteien zur Einstufung der Kreditwürdigkeit von Unternehmen und Privatpersonen überprüft. Die Pressemitteilung vom 05.06.2020 lässt aufhorchen: Nach den Grundsätzen für die Verarbeitung personenbezogener Daten gemäß DSGVO müssen die Daten u. a. „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein“, Art. 5 Abs. 1 lit. d DSGVO. Gegen diesen Grundsatz haben Wirtschaftsauskunfteien offenbar teilweise verstoßen: So wurden Bonitätsbeurteilungen bei nicht vorliegenden Informationen z. B. auf Basis von Annahmen getroffen. Dies führte dazu, dass Kreditrahmen niedriger eingestuft wurden. Bewertungen sind jedoch nur dann rechtmäßig, wenn die Richtigkeit der genutzten Daten (und damit der Bewertung selbst) sichergestellt ist.

Universalität der Grundrechte

Am 19.05.2020 hat das Bundesverfassungsgericht über die Auslandsfernaufklärung des Bundesnachrichtendienstes im Ausland geurteilt und Teile des BND-Gesetzes für verfassungswidrig erklärt. Im Urteil stellt das BVerfG klar, dass sich deutsche Staatsgewalt auch an die Grundrechte (im Verständnis von Abwehrrechten, z. B. zum Schutz vor staatlichen Abhörmaßnahmen) halten muss, wenn sie Wirkungen außerhalb des deutschen Staatsgebietes erzeugt, und auch dann, wenn keine deutschen Bürger betroffen sind.

Dieses Urteil wird bei der Gesetzgebung zu generell grenzüberschreitenden Sachverhalten wie Datenschutz, Rechtsfragen des Internet, Medienrecht usw. künftig stets zu beachten sein. Damit steht es in eklatantem Kontrast zum amerikanischen Grundrechtsverständnis, wie es beispielsweise im US CLOUD Act (SSN 3/2019) zum Ausdruck kommt.

Secorvo News

T.P.S.S.E. und T.I.S.P.

Im September bieten wir Ihnen wieder die Möglichkeit, Ihre Kenntnisse und Kompetenzen in der IT-Sicherheit zu aktualisieren – und zu zertifizieren: für das Teilgebiet des sicheren Software-Engineerings (T.P.S.S.E., **14.–17.09.2020**) und das Zertifikat als Information Security Professional (T.I.S.P., **21.–25.09.2020**). Zur Vorbereitung erhalten Sie nach Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz“, das im vergangenen Herbst in dritter Auflage im dpunkt-Verlag erschienen ist.

Termine zum Vormerken

Am 08.07.2020 bietet KA-IT-Si-Partner Connecting Media die zweite SecurityCruise – diesmal auf der „MS Digital“. Spannende Vorträge, Workshops und spezielle Talkrunden mit den größten IT-Security-Anbietern im deutschsprachigen Raum erwarten Sie. Für KA-IT-Si-Partner und –Unterstützer gibt es das Steuermannpaket zum Vorteilspreis von 45 €. Schicken Sie bei Interesse eine kurze E-Mail an info@ka-it-si.de und wir senden Ihnen den Rabattlink zu.

Derweil freuen wir uns darauf, unsere KA-IT-Si-Veranstaltungen im zweiten Halbjahr 2020 wieder aufzunehmen. Notieren Sie sich gerne schon einmal die geplanten Termine in Ihrem Kalender: 24.09.2020 | 22.10.2020 | 12.11.2020 | 10.12.2020. Wir beginnen im September mit einem spannenden Vortrag zum „Mythos der Enigma“ von Johann Grathwohl, IT-Security-Architekt bei CONITAS.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2020	
08.07.	Security Cruise (Connecting Media, Karlsruhe)
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)
August 2020	
01.-06.08.	Blackhat USA 2020 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
07.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
17.-21.08.	Crypto 2020 (IACR, Santa Barbara/US)
September 2020	
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)

Fundsache

Das *Border Gateway Protocol* (BGP) ist ein zentraler Bestandteil des Internet-Routings. Wie unsicher BGP ist, haben in den letzten Jahren verschiedene „Fehlkonfigurationen" z. B. von chinesischen, pakistanischen oder russischen Internet Service Providern gezeigt. Cloudflare hat mit der Website „Is BGP Safe Yet?" am 17.04.2020 eine Art „digitalen Pranger" eingerichtet, der ISPs animieren soll, Sicherheitsmechanismen wie die kryptographische Validierung von Routing-Informationen zu nutzen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de