Secorvo Security News

Juni 2021

Erpressbar

Ransomware-Angriffe, bei denen die Daten der Opfer verschlüsselt und erst nach Zahlung eines Lösegelds wieder zur Entschlüsselung freigegeben werden, sind in den vergangenen Monaten zu einem beachtlichen Unternehmensrisiko herangewachsen. So hat nicht nur die Zahl der Angriffe, sondern auch die Höhe der Lösegeldforderungen erheblich zugenommen.

Seit etwa zehn Jahren sind Ransomware-Angriffe verbreitet. Da die Angreifer häufig genug Lösegeldzahlungen von den betroffenen Unternehmen erhalten, sind die Angriffe nicht nur finanziell sehr attraktiv, sondern werden auch erhebliche Summen in die Weiterentwicklung der Angriffssoftware investiert.

Die von einem Angriff betroffenen Unternehmen und Institutionen sind dabei allerdings nicht nur Opfer eigener Versäumnisse wie unzureichender Schutzmaßnahmen, fehlender Updates oder lückenhafter Backup- und Notfall-Konzepte, sondern auch der Schwachstellen in erworbener Software: Gäbe es diese Lücken nicht, wären Ransomware-Angriffe vergleichsweise selten erfolgreich.

Dennoch sind Schadensersatzforderungen an diese „Mitverursacher" schwierig, denn die Angreifer verwischen ihre Spuren: Meist ist nicht oder nur mit sehr viel forensischem Aufwand feststellbar, auf welchem Weg das Eindringen in die Systeme gelungen ist. Kein Wunder, wollen die Täter ihr technisches Vorgehen doch noch bei weiteren Opfern erfolgreich praktizieren – und obendrein die von ihnen entwickelte Angriffssoftware vor „Piraterie" schützen.

Damit bleibt Unternehmen und Behörden nur eines: Sich darauf einzustellen, dass – allen Schutzmaßnahmen zum Trotz – ein Ransomware-Angriff passieren kann. Und dafür zu sorgen, dass Angriffe schnell erkannt werden, Backups nicht verschlüsselt werden und ein Neuaufsetzen der Infrastruktur in kurzer Zeit gelingt. Diesen Weg sollte nur scheuen, wer über ausreichend Rücklagen verfügt.

Security News

Konzertierte Aktion

Die deutschen Datenschutz-Aufsichtsbehörden haben am 02.06.2021 die Durchführung einer koordinierten Prüfung internationaler Datentransfers personenbezogener Daten angekündigt. Damit soll den Anforderungen des Europäischen Gerichtshofs aus seiner Schrems-II-Entscheidung vom 16.07.2020 zur Durchsetzung verholfen werden: So dürfen weder das „Privacy Shield" noch die Standardvertragsklauseln ohne „wirksame zusätzliche Maßnahmen" als Rechtsgrundlage herangezogen werden.

Dazu werden ausgewählte Unternehmen zunächst mit abgestimmten Fragebögen zu Bewerberportalen, konzerninternem Datenverkehr und Tracking angeschrieben; außerdem stehen Mailhoster und Webhoster auf der Liste der Aufsichtsbehörden. Auch wenn zunächst nur ein (geringer) Teil der rund 3,3 Mio. deutschen Unternehmen angeschrieben werden wird, lohnt ein Blick in die Fragebögen, die u. a. von der Webseite des virtuellen Datenschutzbüros abgerufen werden können: Sie zeigen, welche Prüfpunkte im Fokus der Aufsichtsbehörden stehen.

Parallel-Welten-Netze

Seit einiger Zeit werden über "LoRaWAN" (Long Range Wide Area Network) IoT-Geräte über Funkverbindungen mit kleiner Reichweite zu Weitverkehrsnetzen mit geringer Bandbreite zusammengeschlossen. Am 08.06.2021 aktivierte Amazon USA ein bereits 2019 angekündigtes neues Feature von Amazon-Echo- und -Ring-Geräten, das diese LoRaWAN-Technik in Kombination mit BLE (Bluetooth Low Energy) nutzt: Bei schlechter Verbindung zum eigenen WLAN verbinden sich Amazon-Geräte via Amazon Sidewalk nun automatisch mit anderen Amazon-Geräten in der Umgebung, um eine Netzverbindung zu erhalten. Konkret redet der eigene Amazon-Lautsprecher oder die Ring-Kamera dann nicht mehr mit dem gerade schlecht verfügbaren WLAN-Router, sondern z. B. mit dem Echo-Gerät des Nachbarn. Dieses fungiert als „Bridge" zum Internet und stellt dafür 80 kbit/s seiner Bandbreite zur Verfügung.

Ähnliche Ansätze gab es bereits in der Vergangenheit mit Hotspots einiger ISPs. Dabei stellten private Router zusätzlich ein Gastnetzwerk zur Verfügung, über das andere Kunden desselben Providers Zugriff zum Internet erhielten. Der große Unterschied liegt allerdings darin, dass derartige Hotspots durch ein dediziertes Netzwerk-Gerät aufgespannt werden (Router), das über entsprechend segmentierende Sicherheitsfunktionen dafür sorgt, dass die Nutzer des Hotspots den eigenen Geräten nichts anhaben können.

Ob sich Lautsprecher und Kameras als Netzwerk-Barrieren eignen, sollte trotz ggf. sogar guter Spezifikation gründlich getestet werden. Und selbst dann stellt die reine Bereitstellung der Schnittstelle einen neuen Angriffsweg dar. Sobald die Funktion auch in Deutschland aktiviert wird, sollte man daher entscheiden, ob man Pioniernutzer dieser neuen Lösungen sein möchte – oder die Option in der Konfiguration lieber deaktivieren.

Alles auf Anfang

Von der Europäischen Kommission wurden am 04.06.2021 neue Standardvertragsklauseln für die DSGVO-konforme vertragliche Regelung des internationalen Austauschs personenbezogener Daten beschlossen und vom Europäischen Parlament verabschiedet. Darin wurde der durch die Cookies-II-Rechtsprechung entstandene Änderungsbedarf berücksichtigt.

Auch wenn die bisher gültigen Standardvertragsklauseln noch bis Ende September 2021 abgeschlossen werden können, ist es wichtig zu wissen, dass diese

nur noch bis Ende Dezember 2022 verwendet werden dürfen. Bis dahin müssen sämtliche Verträge auf die neuen Standardvertragsklauseln umgestellt sein.

Zoom-Benchmark

Das Center for Internet Security (CIS) ist bekannt für Hardening Guides/Benchmarks zu Betriebssystemen, Webservern oder Datenbanken. Inzwischen gibt es auch Guides für Anwendungen und Cloud-Lösungen wie Zoom oder Azure – denn auch Cloud-Dienste sollte man restriktiv konfigurieren. Die Benchmarks sind in der Regel recht ausführlich und unterscheiden die Anforderungen u. a. nach Level 1 und Level 2. Einstellungen des Level 1 sollten in den meisten Fällen problemlos umsetzbar sein; bei Level 2 ist ggf. je Einstellung im Einzelfall eine Prüfung erforderlich.

Zur automatisierten Prüfung werden vom CIS mit Kosten verbundene Werkzeuge bereit gestellt: für den regelmäßigen Einsatz und wiederholte Compliance-Prüfungen eine gute Lösung. Testen kann man dies bspw. für Zoom über Test-Skripte, die Ende Mai 2021 auf Github zur Verfügung gestellt wurden.

Bann für Banner

Am 31.05.2021 hat die Stiftung noyb (my privacy is None of YOur Business) von Datenschutzaktivist Max Schrems den Cookie-Bannern pressewirksam den Kampf angesagt. Allen Cookie-Bannern? Nein, nur solchen, die genervten Nutzern nicht die richtigen Auswahlmöglichkeiten lassen. noyb will über 500 Unternehmen anschreiben, bei denen nicht rechtmäßige Cookie-Banner festgestellt wurden, und droht mit einer Datenschutzbeschwerde bei der zuständigen Aufsichtsbehörde.

Da Webseiten nur selten korrekte Cookie-Banner verwenden, könnte eine beträchtliche Anzahl von weiteren Beschwerden die (von Schrems sicher erhoffte) Folge sein. In der Regel werden mindestens die Anforderungen an den Widerspruch für erteilte Einwilligungen (genauso einfach wie die Erteilung) gar nicht oder nicht korrekt umgesetzt.

Dabei kann man in den Leitlinien des European Data Protection Board nachlesen, wie es richtig geht. Großen Nachbesserungsbedarf sieht auch das ULD bei der länderübergeifenden Datenschutz-Prüfung von Medien-Webseiten. Wer es genau wissen will, dem sei der Vortrag „Cookies, Tracking, Analysen“ von RAin Friederike Schellhas-Mende (Secorvo) auf dem kommenden Karlsruher Tag der IT-Sicherheit am 15.07.2021 ans Herz gelegt (siehe unten).

E-Privacy-Richtlinie umgesetzt

Das schon lange erwartete „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG) wurde endlich am 28.05.2021 im Bundestag und tags darauf im Bundesrat beschlossen. Mit diesem Gesetz, das zusammen mit dem novellierten Telekommunikationsgesetz (TKG) am 01.12.2021 in Kraft tritt, wird die E-Privacy-Richtlinie der EU vor allem hinsichtlich der Cookies umgesetzt. Geregelt werden der digitale Nachlass und insbesondere das Thema Cookies und

Einwilligungen. Das Gesetzt enthält in § 25 die Vorgabe, dass eine Einwilligung in das Setzen von Cookies immer dort notwendig ist, wo es sich nicht um technisch notwendige Cookies handelt, die beispielsweise zum Betrieb der Webseite erforderlich sind. Interessant ist § 26, in dem die Grundlage für Einwilligungsverwaltungsdienste gelegt wird. Diese Regelung muss aber noch mittels einer Verordnung konkretisiert werden.

Bei der Umsetzung sollte beachtet werden, dass nicht alles, was für den Nutzer komfortabler auch besser ist: Die Möglichkeit zur zentralen Speicherung und Verwaltung von Einwilligungen bei Treuhändern erscheint verlockend, bringt aber neue Risiken mit sich. Auch die Einwilligung über Voreinstellungen des Internetbrowsers sollte sehr kritisch betrachtet werden, wenn man eine Eindämmung der Bannerflut erreichen will. Völlig außer Acht geblieben sind leider die Anforderungen an die Gestaltung der Cookie-Banner; hier ist erster Nachbesserungsbedarf erkennbar.

Secorvo News

Teamverstärkung

Seit dem 01.07.2021 verstärkt Milan Burgdorf, Diplom-Jurist mit mehrjähriger Berufserfahrung als Informationssicherheitsbeauftragter das Secorvo-Team. Herzlich willkommen!

Secorvo Seminare

Nachdem die Infektionszahlen erwarten lassen, dass im Spätsommer die Durchführung von Präsenzseminaren wieder möglich sein wird, bieten wir das erfolgreiche T.I.S.P.-Seminar vom **20.09. bis 24.09.2021** (schnelle Buchung empfohlen) und vom **22.11. bis 26.11.2021** an. Das Programm und die Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

12. Tag der IT-Sicherheit

Der jährliche "Karlsruher Tag der IT-Sicherheit", eine Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V., findet in diesem Jahr als virtuelle Veranstaltung statt – verteilt auf drei Abende. Der erste Abend mit Prof. Dr. Jörn Müller-Quade (Leiter der Forschungsgruppe „Kryptografie und Sicherheit“ am KIT) und dem White-Hat-Hacker Tim Schmidt am 01.07. stieß bereits auf großen Zuspruch. Es folgen:

2. Abend – Donnerstag, **08.07.2021**, 18 Uhr

Einfach.Sicher.Machen. Transferstelle IT-Sicherheit im Mittelstand. *Stephanie Ziegler (KIS)*

Modernes DNS: Datenschutz mit Nebenwirkungen.
Prof. Dr. Rainer W. Gerling

3. Abend – Donnerstag, **15.07.2021**, 18 Uhr

Elevator Pitch: StartUps IT-Security.
Jun.-Prof. Dr. Christian Wressnegger (Poison Ivy) und *Mirko Ross (asvin)*

Cookies, Tracking, Analysen.
Friederike Schellhas-Mende (Secorvo)

Im Anschluss an die Vorträge bieten wir die Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit den Referenten und anderen Teilnehmern. Wir freuen uns auf drei kurzweilige und interessante Abende mit Ihnen! (Anmeldung)

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2021	
01.07.	12. Tag der IT-Sicherheit, 1. Abend (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
08.07.	12. Tag der IT-Sicherheit, 2. Abend
12.-14.07.	PETS 2021 (University of Minnesota, virtuell)
12.-16.07.	DFRWS USA 2021 (DFRWS, virtuell)
15.07.	12. Tag der IT-Sicherheit, 3. Abend
31.07.-05.08.	Blackhat USA 2021 (Blackhat, Las Vegas/US)
August 2021	
05.-09.08.	DEF CON 29 (DEFCON, Las Vegas/US)
08.-10.08.	SOUPS 2021 (usenix, Vancouver/CAN)
11.-13.08.	30th USENIX Security Symposium (usenix, Vancouver/CAN)
15.-19.08.	Crypto 2021 (IACR, Santa Barbara/US)
September 2021	
07.-09.09.	6th IEEE European Symposium on Security and Privacy (IEEE, Wien/AUT)
14.-15.09.	D•A•CH Security (Institut für Verteilte Intelligente Systeme, syssec, München)
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)

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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.