Secorvo Security News

Juli 2021

Die Bäume und der Wald

Je tiefer wir in den Schutz der immer komplexeren Informationstechnik eintauchen, desto eher laufen wir Gefahr das große Bild aus den Augen zu verlieren. Treten wir also einen Schritt zurück.

Besonders zwei Entwicklungslinien sind es, die sich gerade deutlich abzeichnen. Die eine: Mit der zunehmenden Digitalisierung entstehen zahlreiche neue Risiken, die oft erst nach einem Vorfall erkannt werden, so wie Anfang Juli beim Ransomware-Vorfall im Landratsamt Anhalt-Bitterfeld. Der Landrat rief den Katastrophenfall aus: Wochenlang konnten im Landkreis weder Wohngeld noch Sozialhilfe gezahlt, Mitarbeitergehälter überwiesen oder Fahrzeuge angemeldet werden.

Die zweite Entwicklungslinie zeigt, wie wenig wir bisher der ersten gewachsen sind – und wie unverstanden der Zusammenhang noch ist. Denn wie in einer Parallelwelt zeigte die CDU die Forscherin Lilith Wittmann beim LKA an, nachdem diese am 11.05.2021 eine hoch kritische Sicherheitslücke in der CDU-Connect-App entdeckt und dem CERT-Bund gemeldet hatte. Schon am 18.05.2009 wies das BVerfG eine Beschwerde gegen den „Hackerparagrafen" § 203c StGB zurück, der immer wieder die bspw. datenschutzrechtliche Ahndung der Verbreitung von Programmen mit Sicherheitslücken verhindert –wie sollte man auch eine solche Lücke dokumentieren, ohne ein Programm zu verwenden, das sie ausnutzt? Und am 08.06.2021 lehnte es eine Beschwerde gegen die Geheimhaltung von Zero-Day-Exploits durch deutsche Sicherheitsbehörden ab – genau damit entwickelt die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) seit 2017 Software zur Telekommunikationsüberwachung.

Klar ist: Unsere Zukunft wird digital sein. Funktionieren wird sie nur, wenn sie sicher ist. Daher muss die systematische Beseitigung von Sicherheitslücken unser aller Ziel sein. Auch das der Sicherheitsbehörden. Die Geheimhaltung und Verbreitung solcher Lücken gehört geahndet – nicht deren Aufdeckung oder Dokumentation.

Security News

UK ist sicheres Drittland

Aufatmen in vielen Unternehmen: Entgegen den Bedenken des EU-Parlaments hat die EU-Kommission am 28.06.2021 den Angemessenheitsbeschluss für Großbritannien (UK) angenommen. Damit gilt UK nun als sicheres Drittland mit angemessenem Datenschutzniveau, obwohl der Investigatory Powers Act dem britischen Geheimdienst ähnlich viele Befugnisse einräumt wie den US-amerikanischen Diensten der FISA 702, der EO 12333 und der CLOUD Act. Die UK-

GDPR basiert auf den europäischen Standards und übernimmt wesentliche Teile der DSGVO. Darin enthalten sind aber auch Ausnahmeregelungen zu Zwecken der Einwanderungskontrolle, was neben den unkontrollierten Zugriffen durch die Geheimdienste für Bedenken gesorgt hat.

Der Angemessenheitsbeschluss hat eine Laufzeit von sechs Jahren, kann aber durch die Kommission jederzeit eingeschränkt oder auch komplett aufgehoben werden.

Ransomware-Hotfix

Am 02.07.2021 gelang es Angreifern der Ransomware-Gruppe REvil mittels einer Zero-Day-Schwachstelle zahlreiche Installationen der Softwareverteilungsplattform Kaseya VSA zu kompromittieren. Die Cloud-Plattform des Herstellers konnte offenbar rechtzeitig abgeschaltet werden; die On-Premise-Instanzen diverser Kunden wurden jedoch übernommen und lieferten eine als Hotfix getarnte Ransomware an die verwalteten Systeme aus. Die Erpresser forderten anschließend von Kaseya die Rekordsumme von 70 Mio. Dollar für die Entschlüsselung der betroffenen Systeme. Bei vielen Unternehmen kam es zu Einschränkungen des IT-Betriebs.

Der Angriff veranlasste US-Präsident Joe Biden, Wladimir Putin am 09.07.2021 aufzufordern, gegen die mutmaßlich aus Russland stammende Gruppe REvil vorzugehen. Offenbar gerieten die Angreifer unter Druck: Am 05.07.2021 senkten sie ihre Forderung überraschend auf 50 Mio. Dollar, und am 13.07.2021 verschwanden ihre Webseiten. Ob die Gruppe untergetaucht ist oder ob es sich um eine Aktion der Ermittlungsbehörden oder der Geheimdienste handelt, ist nicht bekannt. Allerdings teilte Kaseya am 23.07.2021 mit, dass man von einer „vertrauenswürdigen Drittpartei" einen Generalschlüssel erhalten habe.

In den vergangenen Jahren erfolgen vermehrt Angriffe über die „Supply Chain", so wie der Solarwinds-Hack vom vergangenen Dezember. Bei solchen Angriffen werden mit einer Schwachstelle zahlreiche Kunden gleichzeitig kompromittiert, trotz ansonsten angemessener Schutzmaßnahmen. Daher sollte für administrative Werkzeuge ein besonders hohes Schutzniveau greifen.

Ransomware Readiness

Am 30.06.2021 veröffentlichte die amerikanische Cybersecurity & Infrastructure Security Agency (CISA) ein neues Modul für das Cyber Security Evaluation Tool (CSET). CSET ist eine Desktop-Software für Windows, die umgesetzte Schutzmaßnahmen im Netzwerk prüft. Mit dem neuen Modul Ransomware Readiness Assessment (RRA) wird überprüft, wie gut eine Organisation technisch und organisatorisch vor Ransomware-Vorfällen geschützt ist und ob sie sich von einem Vorfall absehbar erholen kann.

In einem ersten Test machte das Modul einen guten Eindruck – es eignet sich auch für Organisationen, die einen ersten Überblick gewinnen wollen, da sie noch nicht so genau wissen, was beim Thema „Schutz vor Ransomware" zu beachten ist. Vorausgesetzt, man

scheut die Installation einer 1 GB großen EXE-Datei nicht, die einen kompletten Microsoft IIS Express zum Anzeigen einer Webseite mitbringt. Nehmen Sie vorsichtshalber eine virtuelle Maschine – denn auch bei Tests kann man sich etwas einfangen.

Grenzen des One-Stop-Shop

Bisher konnten nationale Aufsichtsbehörden bei angezeigten Verstößen gegen die DSGVO nicht direkt gegen Unternehmen mit Firmensitz in einem anderen europäischen Mitgliedsstaat vorgehen, weil entsprechend Art. 56 DSGVO die Federführung einer solchen Untersuchung bei der Aufsichtsbehörde des Sitzlandes liegt. Im unternehmens- oder steuerrechtlichen Kontext ist dieses Zuständigkeitsprinzip als „One-Stop-Shop" bekannt.

In der Vergangenheit stellte dieses Prinzip beispielsweise die deutschen Aufsichtsbehörden vor erhebliche Probleme, wenn sie mögliche Verstöße von großen Internet-Konzernen untersuchen wollten, die ihren Sitz in Irland haben.

Der EuGH hat nun am 15.06.2021 bestätigt, dass nach Art. 55 DSGVO eine nationale Aufsichtsbehörde einen Verstoß gegen die DSGVO selbst verfolgen kann, sofern sie das Verfahren der Zusammenarbeit und Kohärenz nach Art. 60 DSGVO eingehalten hat. Allerdings – und das ist neu – stellt der EuGH klar, dass die nationale Behörde zur wirksamen Anwendung der DSGVO den angeblichen Verstoß weiter untersuchen darf, wenn die federführende Aufsichtsbehörde nicht mit ihr zusammenarbeitet. Eine lesenswerte Zusammenfassung des Urteils findet sich in der EuGH-Pressemitteilung.

MS PKI under attack

Via Advisory warnte Microsoft am 23.07.2021 vor einem „PetitPotam" getauften NTLM-Angriff auf den Zertifikatsdienst der Microsoft-PKI, mit dem ein Angreifer sich Nutzer-Berechtigungen verschaffen kann. Die Ursache ist – wieder einmal – übertriebene Abwärtskompatibilität: Da Microsoft NTLM per Default-Einstellung unterstützt, dürften von der Schwachstelle sehr viele Microsoft-PKIs betroffen sein. Die wirksamste (und simpelste) Schutzmaßnahme ist daher auch, die NTLM-Authentifikation mindestens auf Domain-Controllern zu deaktivieren – ohnehin eine gute Idee, um sich vor weiteren noch unentdeckten Bugs zu schützen. Falls das nicht gewünscht ist, sollte man zumindest den Web-Enrollment-Dienst der Windows-PKI deaktivieren oder ihm, wenn er gebraucht wird, NTLM verbieten. Der PKI-Experte Hans-Joachim Knobloch (Secorvo) beschreibt nach seiner ausführlichen Untersuchung des Angriffs vom 28.07.2021 was dafür zu tun ist.

Dabei entdeckte er einige weitere beunruhigende Varianten. Denn Zertifikate können auch über den Network Device Enrollment Service (NDES) angefordert werden. Dabei kann es einem Angreifer je nach Konfiguration der PKI gelingen, ein Kerberos-Ticket zur Anmeldung am Domain-Controller mit administrativen Berechtigungen zu erschleichen. Hans-Joachim Knobloch listet in seinem Blog-Beitrag vom 30.07.2021

zahlreiche Maßnahmen, die vor dieser Attacke wirksam schützen.

Ersatz für Cookie-Banner?

In Kooperation mit den Sustainable Computing Labs der Wirtschaftsuniversität Wien möchte die NGO noyb die allgegenwärtigen Cookie-Banner durch Advanced Data Protection Control (ADPC) ersetzen. Die Idee veröffentlichte Max Schrems am 14.06.2021: Durch ein automatisches Browser-Signal soll der Nutzer eine Einwilligung erteilen oder verweigern, eine bereits erteilte Einwilligung widerrufen oder einer Verarbeitung aus einem berechtigten Interesse widersprechen können.

Dafür soll eine hersteller- und browserunabhängige standardisierte Schnittstelle eingeführt werden. Statt eines reinen Ja-Nein-Mechanismus' sollen Nutzer einerseits nach Art der Daten entscheiden und andererseits Entscheidungen für mehrere Webseiten treffen können. So soll auch ein „Opt In" möglich sein, das ein differenziertes Einwilligungsmanagement bietet. Dieser Ansatz sollte auch beim Einwilligungsmanagement nach § 26 TTDSG berücksichtigt werden (siehe SSN 6/2021). Für Firefox und Chromium-basierte Browser existieren bereits Prototypen.

Secorvo News

Septemberseminare

Endlich sind Präsenzseminare wieder ohne Bedenken möglich. Daher können wir Sie vom **20. bis 24.09.2021** wieder auf die berufsqualifizierende, angesehene T.I.S.P.-Zertifizierung vorbereiten. Nach Ihrer Anmeldung erhalten Sie vorab unser T.I.S.P.-Buch zugesandt (Amazon-Rating: 4,8).

Da wir während der Pandemie gelernt haben, dass Online-Formate sich besonders für eintägige Hands-On-Seminare eignen, bieten wir erneut am **15.09.2021** unser Live-Hacking-Lab online an. Und vom **28. bis 30.09.2021** stellen wir Ihnen mit IT Security Insights aktuelle Themen der IT-Sicherheit vor (als T.I.S.P.-Update anerkannt).

Alle Programme und die Möglichkeit zur Online-Anmeldung finden Sie auf unseren Webseiten.

Irren ist kryptografisch

Die Kryptoanalyse der ENIGMA ist eine der spannendsten Geschichten in der Kryptografie. Bis in die 70er Jahre wurde in der Öffentlichkeit – und nicht nur dort – angenommen, dass die wichtigste Verschlüsselungsmaschine des zweiten Weltkriegs nicht geknackt worden war. Ein Irrtum: Die ENIGMA wurde bereits in den 30er Jahren erfolgreich analysiert, und während des Krieges wurden in Bletchley Park (GB) Nachrichten deutscher U-Boote systematisch entschlüsselt.

Auf dem kommenden KA-IT-Si-Event am 30.09. 2021 wird Johann Grathwohl (IT-Security-Architekt bei CONITAS) die Entwicklung und die historischen Hintergründe der ENIGMA vorstellen und ihre Funktionsweise erläutern. Anschließend wird er die Kryptoanalyse skizzieren und auf Schwachpunkte und Fehler im Design des Verschlüsselungsverfahrens eingehen und

daraus einige wichtige Erkenntnisse für den Entwurfsprozess ableiten.

Wir freuen uns darauf, unsere KA-IT-Si-Events ab September wieder als Präsenzveranstaltungen durchführen und Ihnen unser „Buffet-Networking" zum persönlichen Austausch anbieten zu können. Um die Vorträge auch weiterhin so vielen Interessenten wie in den vergangenen Monaten zugänglich zu machen, werden wir auch eine Teilnahme per Livestream ermöglichen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

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)
16.-20.08.	Crypto 2021 (IACR, virtuell)
September 2021	
06.-10.09.	6th IEEE European Symposium on Security and Privacy (IEEE Computer Society, virtuell)
13.-16.09.	European Identity & Cloud Conference 2021 (KuppingerCole, München)
20.-24.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
27.09.-01.10.	Informatik 2021 (GI, Berlin)
28.-30.09.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
30.09.	Irren ist kryptografisch (KA-IT-Si, Karlsruhe/online)

Fundsache

Am 17.07.2021 hat der Landesbeauftragte für Datenschutz-und Informationsfreiheit in Baden-Württemberg eine Handreichung zur Durchführung von Online-Prüfungen veröffentlicht, nachdem er festgestellt hatte, dass bei zahlreichen Prüfungen von Hochschulen die räumliche und technische Privatsphäre von Studierenden verletzt worden war.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, 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