Secorvo Security News

Juli 2024

Manchmal muss man müssen wollen…

Seit Monaten werden in einschlägigen Medien Drohkulissen aufgebaut, wie sehr die deutschen Unternehmen von neuen Regularien zur Cybersicherheit durch die Umsetzung von NIS-2 geknechtet werden sollen. Man liest sogar, dass Unternehmen bis zum 17.10.2024 schier unerfüllbare Anforderungen umsetzen müssten.

Dabei galt die Oktoberfrist nie für Unternehmen, sondern war eine Frist für den deutschen Gesetzgeber, die EU-Richtlinie NIS-2 in geltendes Recht zu überführen. Nachdem das Bundeskabinett am 24.07.2024 endlich einen Entwurf für das NIS2UmsG beschlossen hat, wird dieser wohl in absehbarer Zeit zu deutschem Recht werden.

Das Gesetz sieht keine Umsetzungsfrist vor, aber die betroffenen ca. 29.500 Unternehmen haben voraussichtlich drei Jahre Zeit, bis sie die Anforderungen nachweisen müssen. Doch zaubert NIS-2 keine überraschend neuen Anforderungen aus dem Hut. Tatsächlich traut der Gesetzgeber der Wirtschaft offensichtlich nicht zu, Cybersicherheit angemessen umzusetzen und fordert daher legislativ, was schon lange als Good Practice gilt. Wer seine Informationssicherheit nach etablierten Standards wie ISO 27001 oder IT-Grundschutz umgesetzt hat, kann den neuen Anforderungen erst einmal gelassen entgegensehen, auch wenn sich die Details der Umsetzungvorgaben noch in der Abstimmung befinden.

Dass die zusätzliche Bürokratie die Cybersecurity in Deutschland faktisch verbessern wird, wage ich zu bezweifeln. Ich wünsche mir, dass Unternehmen, die Cybersecurity bisher stiefmütterlich behandelt haben, die ungeliebten Gesetzesanforderungen nicht nur mit minimalem Aufwand gerade so erfüllen, sondern dass sie die Chance nutzen, sich wirksam vor aktuellen Bedrohungen zu schützen.

Security News

Unschärfen

Andrea Pierini, Sicherheitsforscher und schon im Jahr 2022 auf dem Microsoft Researcher Recognition Program Leaderboard zu finden, berichtete am 12.07.2024, dass er zeitgleich mit einem anderen Forscher eine neue Schwachstelle an Microsoft gemeldet hatte. Während seine Meldung als „mittelschwer" zurückgestellt wurde, führte die andere zu CVE-2024-38061 und der Aufnahme in den Juli-Patchday.

Der Fall belegt, dass die vermeintlich exakte CVSS-Schwachstellenbewertung – eine Kennzahl aus ca.

einem Dutzend Einzelkriterien – eben doch mehr oder minder große Ermessensspielräume zulässt: Ist die Komplexität des Angriffs niedrig oder hoch? Wie schwer wirkt sich ein Integritätsverlust auf nachfolgende Systeme aus?

Dies macht den Vorteil der Komplexitätsreduktion durch eine CVSS-Maßzahl ein Stückweit zunichte. Sicherlich wird man bei 9er- oder 10er-Schwachstellen in der IT-Infrastruktur sofort handeln müssen. Aber zwischen den CVSS-Schwellenwerten für „alles andere stehen und liegen lassen" und „machen wir, wenn Zeit dafür ist" gibt es einen wohl eher breiten Graubereich, in dem man die Einzelbewertungen und deren Relevanz für die eigene Umgebung überprüfen sollte.

Selbstverständlichkeiten

Am 14.06.2024 berichtete der Landesbeauftragte für den Datenschutz Niedersachsen über eine von seiner Behörde vorgenommene anlassunabhängige Datenschutzprüfung, bei der über das Internet erreichbare Microsoft-Exchange-Server niedersächsischer Unternehmen auf Verwundbarkeiten untersucht wurden. Dabei wurden 20 Server mit kritischen Schwachstellen gefunden. Die Aufsichtsbehörde wertet das Fehlen aktueller Patches als Verstoß gegen die Pflicht, die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten (Art. 32 DSGVO). Statt eines Bußgelds erhielten die Unternehmen allerdings nur eine Verwarnung.

Schon am 26.03.2024 hatte das BSI berichtet, dass mindestens 17.000 öffentlich erreichbare Microsoft-Exchange-Server kritische Schwachstellen besitzen. Offenbar kümmern sich einige Organisationen nicht um die Aktualisierung ihrer direkt am Internet betriebenen Exchange-Server, die oft einen Zugang über Outlook Web Access (OWA) oder IMAP4 bieten. Beides verwendet in der Regel nur eine Passwortauthentifizierung.

Die verwarnten niedersächsischen Unternehmen haben inzwischen die seit 2021 bekannten Sicherheitslücken durch Patches geschlossen. Wenn man nicht zu Microsoft in die Cloud wechseln möchte, sollte man daher ein E-Mail-Gateway vorschalten und für den Clientzugriff eine VPN-Lösung mit starker Authentifizierung verwenden.

Unverträglichkeiten

„Legacy" und „Kryptoverfahren" sind zwei Begriffe, die sich nicht gut vertragen. Das war so bei der Erzeugung von (EC)DSA-Nonces in PuTTY (siehe SSN 05/2024). Und es ist so bei der Authentisierung von Nachrichten zwischen einem Switch oder Access-Point und dem RADIUS-Authentifikationsserver. Dabei wird seit Mitte der Neunzigerjahre ein Keyed-MD5-Hash verwendet. Dass das nicht der Weisheit letzter Schluss ist, weiß man spätestens seit den Angriffen auf MD5 (1996) und der Standardisierung der HMAC-Konstruktion (1997). Dennoch behielt man das Verfahren bei, weil die Schwachstelle vermeintlich schwer ausnutzbar war und es keine praktischen Angriffe gab.

Am 09.07.2024 veröffentlichte nun ein internationales Forscherteam den praktisch umsetzbaren Blast-RADIUS-Angriff. Damit kann ein Man-in-the-Middle-

Angreifer eine Authentifizierungsanfrage stellen, deren erwartungsgemäße Ablehnung durch den RADIUS-Server er zu einer „authentischen" Akzeptanz umändern kann. Als Reaktion wird nun der RADIUS-Standard überarbeitet, um RADIUS-Nachrichten per TLS/DTLS zu schützen. Das ist seit 2012 bzw. 2014 in den „experimental" RFCs 6614 und 7360 vorgesehen, die auch von einigen Herstellern implementiert wurden.

Bei Legacy-Kryptoverfahren sollte man eher früher als später zu Nachfolgern wechseln – bevor die Hoffnung, dass es schon irgendwie gut gehen wird, durch praktikable Angriffe ein jähes Ende findet.

Vertrauenswürdigkeiten

Google hat am 27.06.2024 angekündigt, dass der Chrome-Browser ab Version 127 keinem Zertifikat mehr vertraut, das auf die Root-CAs von Entrust und AffirmTrust zurückgeht und nach dem 31.10. 2024 ausgestellt wird. Google begründet diesen Schritt mit einer langen Liste von Verfehlungen seitens Entrust, wie verzögert vorgelegte Berichte, schuldhaftes Ausbleiben von Zertifikatrückrufen und Verwendung von unzulässigen Zeichen in Zertifikatseinträgen. Mangels hinreichender Aussicht auf Besserung greife Google nun zu dieser Maßnahme.

Schon öfter hat Google Trust-Center aus eigenen Root-Stores verbannt: 2015 Symantec/Verisign aus Chrome und Android – Mozilla (Firefox) und Apple (Safari) zogen kurz darauf nach. 2021 flog Camerfirma aus Chrome, 2023 TrustCor und im Mai 2024 Globaltrust. Dokumentiert und nachverfolgt werden Verfehlungen über Bugzilla bei der Mozilla Foundation.

In diesem Zusammenhang ist Bug 1877388 vom 29.01.2024 interessant, der die Deutsche Telekom betrifft. Auslöser war ein Verzug bei der Sperrung mehrerer nicht ganz dem vorgegebenen Profil entsprechender Zertifikate. Die Telekom begründet die Verzögerung damit, dass die betroffenen Kunden wichtige Infrastrukturen betreiben und nicht in der Lage sind, die Zertifikate rechtzeitig auszutauschen. Im Laufe der Diskussion mit den Aufsehern der Browser-Hersteller wurden grundsätzliche Fragen aufgeworfen, darunter solche über die personellen Kapazitäten der Telekom.

CAs in den Root-Stores müssen dauerhaft vertrauenswürdig sein. Daher ist es wichtig, Verstöße zu verfolgen, die die Vertrauenswürdigkeit beeinträchtigen. Dabei dürfen aber keine unterschiedlichen Maßstäbe angelegt werden – sonst steht irgendwann das Vertrauen in die Zertifikatsinfrastruktur als Ganze in Frage.

Örtlichkeiten

Netzpolitik.org und Bayrischer Rundfunk (BR) haben am 16.07.2024 Hintergründe zum Handel mit Standortdaten aufgedeckt: Databroker bieten die Datensätze auf Online-Marktplätzen an, sogar als Abo, das stündlich Updates der Nutzerdaten liefert – ein Milliardengeschäft. Die Daten werden vor allem von Apps geliefert, die neben Nutzungsdaten auch Standortinformationen erfassen, und ließen sich mühelos über einfache Online-Recherchen natürlichen Personen zuordnen.

Geschäftsmodelle mit eindeutigen Werbe-IDs und Kategorisierungen sind lange bekannt (siehe z. B. SSN 5/2022). Mit Standortdaten können jedoch Bewegungs-Profile erstellt werden, die Rückschlüsse auf Arbeitsplatz, politische oder religiöse Überzeugungen und Arztbesuche zulassen. Inzwischen läuten auch bei amerikanischen Senatoren die Alarmglocken: Bewegungsdaten können auch verdeckte Ermittler und Geheimdienstmitarbeiter enttarnen.

Wie man seine Werbe-ID zurücksetzt, erläutern Netzpolitik.org, BR und Heise. Zur Erstellung von Nutzerprofilen werden jedoch auch andere Identifikatoren verwendet, die später eine Zuordnung und Zusammenführung der Bewegungsdaten ermöglichen können. Offenbar schrecken drohende Datenschutzbußgelder die Anbieter nicht ab – bleibt als letzte Instanz der Gesetzgeber, um solche Grundrechtsverstöße wirksam zu unterbinden.

Nebensächlichkeiten

Wenn ein Hersteller neue KI-basierte Cloud-Dienste implementiert, werden offenbar gelegentlich eher herkömmliche Aspekte wie Netzwerksicherheit, Firewalling oder der Umgang mit Credentials zu vermeintlichen Nebensächlichkeiten.

So wurde am 17.07.2024 ein Angriff auf den SAP AI Core Dienst unter dem Namen SAPwned veröffentlicht, der sich zunutze macht, dass der Anwender einen Prozess unter der User-ID des integrierten Istio-Proxys starten konnte – und die ist von den IP-Firewall-Regeln ausgenommen. Nach Überwindung dieser Hürde konnte ein Angreifer auf Credentials und offene Dienste zugreifen, mit denen er praktisch die gesamte Cloud-Umgebung übernehmen konnte.

Merke: Insbesondere bei *-as-a-Service darf die Software-Sicherheit nicht beim Code aufhören – auch Deployment und Konfiguration sind sicherheitskritisch und müssen beachtet werden.

Secorvo News

Fachseminare

Haben Sie noch Spielraum im Weiterbildungsbudget? Dann werfen Sie doch einen Blick auf unsere Fachseminare im Herbst. So bereiten wir Sie vom **23. bis 27.09.2024** mit unserem T.I.S.P.-Seminar auf die Zertifizierung als Informationssicherheitsexperte vor, und vom **15. bis 17.10.2024** bilden wir Sie zum Vorfall-Experten nach dem Curriculum des BSI aus. Wir freuen uns auf Ihre Anmeldung.

Weitere Informationen und die Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

Wer die Wahl hat…

Wahlen und Abstimmungen – in Vereinen, Organisationen, Gemeinden, Land und Bund – sind organisatorische und manchmal auch logistische Herausforderungen. Was liegt da näher, als sie zu „digitalisieren“?

Beim KA-IT-Si-Event am **12.09.2024** beleuchtet Frau Professorin Melanie Volkamer (Secuso, KIT) die Sicherheitsanforderungen an Internet-Wahlen und -

Abstimmungen, stellt praktische Beispiele vor und diskutiert die Vor- und Nachteile ihres Einsatzes.

Anschließend erwartet Sie natürlich der Erfahrungsaustausch beim „Buffet-Networking". Wir freuen uns darauf, Sie in der „Church" des CyberForum zu sehen – und empfehlen wie immer eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2024	
03.-08.08.	Blackhat US 2024 (Blackhat, Las Vegas/US)
08.-11.08.	Defcon 32 (DEFCON, Las Vegas/US)
11.-13.08.	SOUPS 2024 (usenix, Philadelphia/US)
14.-16.08.	33nd USENIX Security Symposium (usenix, Philadelphia/US)
18.-22.08.	Crypto 2024 (IACR, Santa Barbara/US)
September 2024	
04.-05.09.	Annual Privacy Forum 2024 (ENISA, DG Connect and Karlstad University, Karlstad/SWE)
11.-12.09.	secIT digital (Heise Medien, virtuell)
12.09.	KA-IT-Si-Event „Wer die Wahl hat..." (KA-IT-Si, Karlsruhe)
12.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
19.-20.09.	37. Kryptotag (GI, Nürnberg)
23.-27.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
25.-26.09.	heise DevSec 2024 (iX, heise Security, dpunkt.Verlag, Köln)

Fundsache

Der Orientierungshilfen-Navigator des LfDI Baden-Württemberg gibt einen Überblick über die Orientierungshilfen zu den datenschutzrechtlichen Implikationen der KI-Verordnung.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Paul Blenderman, Robert Eitel, Kai Jendrian (Editorial), Hans-Joachim Knobloch, Oliver Oettinger, Friederike Schellhas-Mende, Jochen Schlichting, Markus Toran

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