Secorvo Security News

April 2024

Keine Zauberei

Warum gelingen immer mehr Angriffe auf IT-Infrastrukturen von Behörden und Unternehmen? Werden Cyberkriminelle gefährlicher, kompetenter, offensiver? Oder besitzen die IT-Systeme immer mehr Schwachstellen?

Wer die Ursachen erfolgreicher Angriffe analysiert, stellt fest, dass weder das eine noch das andere zutrifft. Zwar hat das Geschäftsmodell „Erpressung" Angreifern einen Schub verpasst – aber das liegt schon über acht Jahre zurück. Und Schwachstellen, die nach wie vor entdeckt werden, ermöglichen immer seltener gleich die Übernahme ganzer Systeme. Tatsächlich waren die bekannt gewordenen Angriffe bis auf wenige Ausnahmen kein Hexenwerk. Vor allem aber: Die meisten hätten sich durch Maßnahmen vereiteln lassen, die seit Jahrzehnten bekannt sind und längst gängige Praxis sein sollten:

1. *Network Segregation*: Eine strukturierte Aufteilung der über das Netz erreichbaren Server und Peripheriegeräte in VLANs, die konsequente Nutzung von DMZ-Rechnern und ein physikalisch getrenntes Backup-Netz erschweren viele Angriffe deutlich oder machen sie sogar unmöglich.
2. *Complexity Reduction*: Eine große Vielfalt an Systemen und Anwendungen, Betriebssystemvarianten und Geräten erschwert es, Software und Hardware in einem möglichst sicheren Zustand zu betreiben. Wer Komplexität verringert gewinnt Überblick und hat mehr Zeit für Härtung und zügige Updates.
3. *Need to know*: Wer Zugriffsrechte und die Erreichbarkeit von Servern und Peripheriegeräten auf das Erforderliche beschränkt, begrenzt den Schaden, den ein Angreifer anrichten kann – unnötige Admin-Rechte, Schreibrechte, Berechtigungen nach Aufgabenwechsel oder Ausscheiden gehören beschnitten.

IT-Sicherheit ist keine Zauberei. Man muss sie wollen. Und konsequent umsetzen, ohne Sonderlocken – denn ein Einfallstor genügt.

Security News

Lernen aus Fehlern Anderer

Selten berichten Opfer öffentlich über einen erfolgreichen Cyberangriff – dabei ließe sich viel daraus lernen. Daher muss man die British Library für ihren 18-seitigen Cyber Incident Review vom 08.03.2024 loben. Detaillierter noch ist r-tecs 42-seitiger Bericht vom 19.01.2024 über den Angriff auf die Südwestfalen-IT – „vertraulich" klassifiziert, aber öffentlich einsehbar. Und nicht nur für Fachleute hörenswert ist der

sechsteilige MDR-Podcast (06.07.-10.08.2023) über den Vorfall im Landkreis Anhalt-Bitterfeld.

Die Ursachen der drei Vorfälle ähneln sich: unzureichend gesicherter Fernzugriff, keine Netz-Segmentierung, fehlende Offline-Backups, viele Legacy-Systeme und nicht zuletzt Budget- und Personalmangel. Wirksame Schutzmaßnahmen wären in allen drei Fällen möglich gewesen – hoffentlich lassen sich das Behörden und Unternehmen eine Lehre sein.

Keine Ausreden

Am 11.04.2024 hat der Europäische Gerichtshof erneut über immateriellen Schadensersatz bei Datenschutzverstößen entschieden. Die Juris GmbH wollte von der Haftung befreit werden, da der Mitarbeiter, der den Verstoß verursacht hatte, klare Weisungen missachtet hatte. Folgt man dieser Argumentation wäre damit jedoch Art. 82 DSGVO ausgehebelt – ein verantwortliches Unternehmen kann sich nicht vor der Haftung drücken, indem es die Schuld Mitarbeitern zuweist und sich darauf beruft, dass diese Pflichten verletzt hätten.

Unternehmen müssen dafür sorgen, dass gesetzliche Bestimmungen tatsächlich eingehalten werden – Eltern haften für ihre Kinder und Unternehmen für ihre Mitarbeiter.

Know Your Contributor

Die Hintertür in xz Utils, die am 29.03.2024 bekannt wurde (CVE-2024-3094), hätte um ein Haar dramatische Folgen gehabt. Sie wurde durch Zufall vom PostgreSQL-Entwickler und Microsoft-Mitarbeiter Andreas Freund entdeckt, der bei Performance-Messungen Verzögerungen in einer neuen Version der Bibliothek liblzma von 0,5 Sekunden beobachtet hatte. Ursache war eine Hintertür, die unautorisierten Secure-Shell-Zugang (ssh) in solchen Linux-Distributionen wie Debian und Red Hat ermöglicht hätte, die den ssh-Service mit dem Management-Dienst systemd verknüpfen – denn der enthält xz.

Eingebaut hatte die Hintertür ein in das Open-Source-Projekt eingeschleuster Maintainer. Über einen ähnlichen Infiltrationsversuch bei der OpenJS Foundation berichtete am 15.04.2024 die Open Source Security Foundation. Da viele, auch sicherheitskritische Projekte wie sudo nur über wenig Wartungs-Ressourcen verfügen, ist daher nicht auszuschließen, dass es bereits erfolgreich eingeschleuste Hintertüren in Linux-Distributionen gibt.

Um bei Bekanntwerden solcher Angriffe auf die „Software-Lieferkette“ schnell reagieren zu können, müssen Unternehmen, Software-Hersteller und Anwender wissen, welche Software welche Bibliotheken in welchen Versionen nutzt. Dabei helfen sogenannte Software Bill of Materials: Listen, die die Abhängigkeiten der Software dokumentieren und automatisch erstellt werden können – z. B. in dem verbreiteten Format System Package Data Exchange (SDPX), das 2021 als ISO/IEC 5692 genormt wurde.

Hinweispflicht auf Schwachstelle

Am 23.11.2023 entschied das Landgericht Bochum, dass es nicht ausreicht, wenn Hersteller über bekannte Sicherheitslücken eines Produkts auf ihrer Webseite informieren. Geklagt hatte die Verbraucherzentrale Bundesverband gegen den Hersteller eines Funk-Türschlossantriebs, der seine Produkte über Online-Plattformen und Einzelhändler vertreibt. Im August 2022 hatte das BSI eine Warnung der Risikostufe „hoch" nach § 7 BSIG ausgesprochen. Nach Ansicht des Gerichts war der entsprechende Hinweis auf der Produktwebseite irreführend (Art. 5a Abs. 1 UWG), da der Hersteller nicht dafür gesorgt hatte, dass Käufer beim Erwerb des Produkts über die Vertriebspartner von der Sicherheitslücke erfahren.

Staatstrojaner

Der Einsatz staatlicher Überwachungssoftware muss nach dem Urteil des Bundesverfassungsgerichts zur Onlinedurchsuchung vom 27.02.2008 von einem Richter angeordnet werden. Wie oft eine solche Durchsuchung vorgenommen wurde, gibt das Bundesamt für Justiz (BfJ) in einer jährlichen Statistik zur Telekommunikationsüberwachung bekannt. Den am 25.04.2024 vom BfJ veröffentlichten Zahlen kann man entnehmen, dass 2022 wie in den Vorjahren weniger als 20 Anordnungen erfolgten – und eine erfolgreiche Installation des „Staatstrojaners" offenbar nur in einem Teil der Fälle gelang. Im Vergleich mit der (weiter) steigenden Anzahl der Verkehrsdatenabfragen (2022: über 30.000) ist das eine geradezu verschwindend geringe Größe.

Formlose Newsletterabmeldung

Unternehmer müssen der Verwendung ihrer E-Mail-Adresse für die Zusendung von Werbung auch formlos widersprechen können - hat das Landgericht Paderborn am 12.03.2024 entschieden. Anderenfalls drohen den werbenden Unternehmen Schadensersatz- und Unterlassungsansprüche.

Für werbetreibende Unternehmen bedeutet das, dass sie Prozesse einführen müssen, die einen Widerruf unverzüglich umsetzen, auch wenn er nicht über das Kundenverwaltungssystem erfolgt. Das erfordert im Zweifel die Sensibilisierung aller Mitarbeiterinnen und Mitarbeiter mit Kundenkontakt.

Consent or Pay

Am 17.04.2024 bezog der Europäische Datenschutzausschuss (EDSA) zu „Consent-or-Pay"-Modellen Stellung, bei denen Besucher von Webseiten vor die Wahl gestellt werden, ob sie für die Inhalte zahlen oder eine Einwilligung in die Verarbeitung ihrer personenbezogenen Daten erteilen wollen. Oft werden diese Daten anschließend für umfangreiche Werbezwecke mit einer Vielzahl von Werbepartnern verarbeitet.

Eine Einwilligung muss nach Art. 7 Abs. 4 DSGVO freiwillig erfolgen. Das „Consent-or-Pay"-Modell biete jedoch keine echte Wahlmöglichkeit, wenn die Gebühren so hoch sind, dass sie die Nutzer daran hindern, eine freie Wahl zu treffen. Nutzer dürften zudem nicht von Online-Diensten ausgeschlossen werden, die eine

wichtige Rolle spielen oder für die Teilhabe am gesellschaftlichen Leben oder den Zugang zu beruflichen Netzwerken entscheidend sind. Personenbezogene Daten dürften nicht als „handelbare Ware" verstanden werden; auch eine Bündelung verschiedener Zwecke in einer Einwilligung sei unzulässig. Schließlich müsse die Information des Verantwortlichen den Nutzern ermöglichen, den Wert, den Umfang und die Folgen einer Einwilligung vollständig zu verstehen. Als „Standard-Lösung" sei das Modell daher ungeeignet.

Datenschutz-Reifegradmodell

Die Erfüllung der gesetzlichen Anforderungen an den Datenschutz ist eine große Herausforderung in Unternehmen, die aus vielen, insbesondere internationalen Organisationseinheiten bestehen. In Heft 3/2024 der Fachzeitschrift Datenschutz und Datensicherheit (DuD) stellen Dirk Fox (Secorvo) und Ingo Lorenz (Konzerndatenschutzbeauftragter der Hansgrohe SE) ein Reifegradmodell vor, das eine strukturierte Vorgehensweise für den Aufbau und Betrieb eines Datenschutzmanagement-Systems über beliebig viele Organisationseinheiten bietet und zugleich eine differenzierte Bestimmung des jeweils erreichten Datenschutzniveaus ermöglicht.

Secorvo News

Secorvo Seminare

In der Kürze liegt die Würze – auch an den beiden Seminartagen IT-Security Insights – T.I.S.P.-Update am **14. und 15.05.2024** zu aktuellen Themen der Informationssicherheit und des Datenschutzes.

Der TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) vom **10. bis 13.06.2024** bringt Ihnen mit spannenden Vorträgen und interaktiven Workshops die sichere Software-Entwicklung nahe.

Und auf unserem T.I.S.P.-Seminar vom **24. bis 28.06.2024** können Sie Ihre Kenntnisse in der Informationssicherheit und im Datenschutz vertiefen und anschließend zertifizieren lassen. Das Anfang März 2024 in vierter Auflage erschienene Begleitbuch erhalten Sie nach Ihrer Anmeldung.

Los, sag' mir was Du weißt. Alles.

Das Recht auf Auskunft über die Verarbeitung persönlicher Daten ist ein Grundrecht. Durch die zunehmende Sensibilisierung für den Datenschutz stellen immer mehr Betroffene Auskunftsanfragen nach Art. 15 DSGVO – und viele Verantwortliche damit vor Herausforderungen. Denn eine Auskunft muss über alle über eine bestimmte Person verarbeiteten Daten erteilt werden.

Am **16.05.2024** stellen Friederike Schellhas-Mende und Christian Blaicher (Secorvo) beim KA-IT-Si-Event im House of Living Labs (FZI) vor, was eine Auskunft nach aktueller Rechtsprechung konkret umfassen muss und wie man sich darauf vorbereiten kann.

Anschließend erwartet Sie wie immer der Erfahrungsaustausch beim „Buffet-Networking". Wir freuen uns auf Sie – und empfehlen Ihnen eine schnelle Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2024	
07.-08.05.	20. Deutscher IT-Sicherheitskongress (BSI, virtuell)
14.-15.05.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
14.-16.05.	Datenschutztage 2024 (WEKA Akademie, Niedernhausen hybrid)
16.05.	KA-IT-Si-Event „Los, sag'was Du weißt. Alles." (KA-IT-Si, Karlsruhe)
22.-24.05.	25. Datenschutzkongress (EURO-FORUM, Berlin)
26.-30.05.	Eurocrypt 2024 (IACR, Zürich/CH)
28.-29.05.	BvD Verbandstage 2024 (BvD, Berlin)
Juni 2024	
03.-05.06.	Entwicklertag 2024 (VKSI, GI, ObjektForum, Karlsruhe)
04.-07.06.	European Identity & Cloud Conference 2024 (KuppingerCole, Berlin)
10.-12.06.	DuD 2024 (COMPUTAS, Berlin)
10.-13.06.	T.P.S.S.E. (TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.-28.06.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
24.-28.06.	OWASP 2024 Global AppSec (OWASP Foundation, Lissabon/PT)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Paul Blenderman, Robert Eitel, Kai Jendrian, 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