Secorvo Security News

November 2021

Keks-Transparente

Sie nerven. Kaum eine Webseite, die noch ohne Mausklick zu erreichen wäre: Zuerst muss man den „Cookie-Banner“ hinter sich bringen. Schlimmer noch: Seltenst kann man das Tracking mit einem einzigen Klick ablehnen – erst auf einer weiteren Seite, oft nach längerem Scrollen und manchmal erst nach mühseligem Deaktivieren der (rechtswidrig) voreingestellten ungewünschten Datenerhebungen. Dabei versuchen Text, Hervorhebung und Farbe der „Knöpfe“ den Besucher zu einem vorschnellen „Einverstanden“ zu bewegen – „Nudging“ heißt dieser neue Wettlauf zwischen Werbestrategen und genervten Seitenbesuchern.

Die gewählte Cookie-Einstellung wird gespeichert – in einem Cookie natürlich, das bei einer datensparsamen Browser-Konfiguration beim Schließen sorgsam von der Festplatte gelöscht wird. Und beim nächsten Seitenbesuch geht alles wieder von vorne los. Bleiben die Webseiten ohne Banner. Sie sind fast noch schlimmer, denn wer einen Tracker-Alarm in seinem Browser installiert hat, weiß, dass die meisten dieser Seiten einfach ohne Einwilligung tracken. So nagt unvermeidlich der Gedanke im Hinterkopf, dass man diese Seiten eigentlich sofort verlassen müsste.

Kein Wunder, dass viele Menschen ein Ziel für ihren Ärger suchen – und es in der DSGVO finden: einem weiteren Beispiel für ausufernde Brüsseler Regelungsbürokratie. Der britische Kultusminister Oliver Dowden dürfte vielen aus dem Herzen gesprochen haben, als er im August die „Abschaffung der endlosen Cookie-Hinweise“ forderte.

Alles verständlich. Und dennoch Unsinn. Das ist, als würde man fordern, allen Autofahrern, die auf fremden Grundstücken parken wollen, das Fragen um Erlaubnis zu erlassen – weil so viele fragen.

Verursacher der Cookie-Banner ist nicht der Datenschutz. Sondern die hemmungslose Aufdringlichkeit, mit der Webseitenbetreiber unser Nutzerverhalten protokollieren und auswerten.

Security News

Ja, ich will!

Der Bayerische Beauftragte für Datenschutz hat am 01.09.2021 eine Orientierungshilfe zum Thema Einwilligung herausgebracht. Diese ist all denjenigen zur Lektüre zu empfehlen, die sich bei der Verarbeitung personenbezogener Daten auf Einwilligungen stützen. Besonders relevant ist dies bei der Gestaltung von Webseiten, die mehr als nur technisch notwendige Cookies verwenden. Unberücksichtigt bleibt darin leider das am 01.12.2021 in Kraft getretene TTDSG, in dem Einwilligungsmanagement und Einwilligungstreuhänder vorgesehen sind. Dazu sollte man sich zeitnah anderweitig informieren.

Ransomware: Never Ending Story

Am 08.11.2021 schaffte es wieder einmal ein Angriff mit Ransomware in die Tagespresse. Dass es sich bei dem Angriff auf den Media-Saturn-Konzern nicht um einen Einzelfall handelt, kann man live auf der Cyber-bedrohung Echtzeitkarte von Kaspersky beobachten oder dem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland des BSI entnehmen.

Neben einem angemessenen Schutz vor Ransomware und anderer Schadsoftware sollte es auch selbstverständlich sein, Vorkehrungen für die Schadensbegrenzung im Fall einer Infektion zu treffen: Verzicht auf unnötige administrative Berechtigungen, Virenschutz, Einschränkungen von Programmausführungen, Makrosicherheit und ein Backup nach der 3-2-1-Regel gehören dazu. Für dunkle Wintertage empfehlen wir die ausführliche Publikation des BSI zum Thema Ransomware mit sinnvollen weitergehenden Maßnahmen zur Lektüre.

Ich sehe was, was Du nicht siehst

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI) hat am 27.10.2021 Hinweise und eine Handreichung zur praktischen Nutzung von Videokonferenzsystemen veröffentlicht. Gemäß Pressemitteilung will der LfDI keine „detaillierten Hinweise zu allen möglichen Konfigurationen und Vertragsgestaltungen geben", sondern bei der Auswahl und Einrichtung des „richtigen" Systems unterstützen.

Leider gelingt dies der Handreichung nicht. Die einführenden Rahmenbedingungen und Empfehlungen sind möglicherweise für den einen oder anderen Nutzer hilfreich. Problematisch sind jedoch die Hinweise zu den verschiedenen Anbietern: Hier fehlt es an einer einheitlichen Darstellung und an der Bewertung des aktuellen Stands der datenschutzrelevanten Dokumente. Es wird erkennbar, dass keine neutrale Beurteilung stattgefunden hat. Daher sollte man zur Auswahl weitere Dokumente wie etwa den Mindeststandard des BSI zu Videokonferenzdiensten als Checkliste hinzuziehen (s. u.).

Videokonferenz-Mindeststandard

Am 07.10.2021 hat das BSI einen Mindeststandard für Videokonferenzdienste veröffentlicht. Obwohl die BSI-Mindeststandards unmittelbar nur für die Informationstechnik des Bundes gelten, enthalten sie häufig praxisorientierte Hinweise in kompakter Form, die auch für andere Behörden und Unternehmen hilfreich sind. Ohne auf bekannte Videokonferenzprodukte einzugehen, werden typische Sicherheits- und Funktionsanforderungen wie ein Rollenkonzept, Verschlüsselung, Dateiablagen, das Teilen von Bildschirminhalten oder Sicherheitsupdates vorgestellt. Zusätzlich wird darauf aufmerksam gemacht, nicht benötigte Funktionen abzuschalten und die Beschäftigten in die Verwendung und Moderation des Videokonferenz-Tools einzuweisen. Bei Einführung oder Betrieb eines Videokonferenzdienstes kann der Mindeststandard somit als Checkliste verwendet werden, um Informationssicherheitsanforderungen an einen Videokonferenzdienst systematisch umzusetzen.

Kontextfreie MFA

Dass auch eine Multi-Faktor-Authentifikation (MFA) ohne vernünftiges „User-Interface“ schief gehen kann, illustrierte Roger Grimes am 20.10.2021 anhand einiger Beispiele. Darunter ist das eines Vice Präsidenten, der ein Login mehrfach mit einem zugesandten zweiten Faktor bestätigte, obwohl er sich nirgends anmelden wollte – und so Angreifer in die Firma ließ.

Solche Fehler darf man nicht allein dem Nutzer vorwerfen, denn oft fehlt bei der Zusendung des zweiten Faktors der Kontext. Einen Sicherheitsexperten wird eine kontextfreie MFA sicherlich Verdacht schöpfen lassen – einen an „kryptische“ E-Mails von der IT gewöhnten Mitarbeiter aber vielleicht nicht. Verständlichkeit und Nachvollziehbarkeit sind für einen wirksamen Schutz unverzichtbar.

Einmal keine Updates eingespielt…

Im Tätigkeitsbericht der niedersächsischen Aufsichtsbehörde für 2020 wird von einem Bußgeld in Höhe von 65.000 Euro gegen einen Onlineshop-Betreiber berichtet, der seine Shop-Anwendung fünf Jahre lang nicht aktualisierte, obwohl der Softwarehersteller auf erhebliche Sicherheitslücken hingewiesen und eine neue Version bereitgestellt hatte. Wesentlich für die Aufsichtsbehörde war, dass nach Art. 24 Abs. 1 DSGVO Schutzmaßnahmen vom Verarbeiter überprüft und aktualisiert werden müssen und dass die Verwendung aktueller, um Sicherheitslücken bereinigter Software für das Unternehmen nicht unverhältnismäßig gewesen wäre. Auch im Tätigkeitsbericht der baden-württembergischen Aufsichtsbehörde für 2020 findet sich ein Bericht über ein Bußgeld in Höhe von 1,2 Mio. Euro gegen eine Krankenkasse, die Maßnahmen zum Schutz der Daten von Gewinnspielteilnehmern nur unzureichend umgesetzt hatte.

Zur Handlungspflicht bei Kenntnis einer Schwachstelle gibt die Pressemitteilung der baden-württembergischen Aufsichtsbehörde Hinweise, was sie beispielsweise bei der Exchange-Lücke von den Betreibern erwartete.

Die Aufsichtsbehörden tolerieren eine nachlässige Umsetzung von technischen und organisatorischen Maßnahmen nicht, erwarten regelmäßige oder anlassbezogene Überprüfungen und insbesondere das zügige Einspielen von Sicherheitsupdates. Sofern personenbezogene Daten verarbeitet werden, ist Informationssicherheit nach Stand der Technik Pflicht.

Top Hardware-Schwachstellen

Die OWASP Top 10 sind mittlerweile jedem ein Begriff, wenn es um die verbreitetsten Schwachstellen in Web-Anwendungen geht. Dass Sicherheit jedoch gerade im Kontext von IoT auch weit mehr als klassische Web-Anwendungen umfasst, griff am 26.10.2021 die MITRE auf und veröffentlichte die 2021 CWE Most Important Hardware Weaknesses bestehend aus den zwölf bedeutendsten Schwachstellenklassen von Hardware. Dazu zählen beispielsweise schlechte kryptographische Implementierungen, unzureichender Schutz gegen Debugging oder fehlende Funktionen für Firmware-Updates.

Insgesamt haben sich die Common Weakness Enumeration (CWE) in den vergangenen Jahren immer weiter durchgesetzt und sind auch bei uns insbesondere im Pentesting zum Standard für die Kategorisierung von Schwachstellen geworden. So liefert die Datenbank nicht nur allgemeine Informationen zur Schwachstelle und Beispiele, sondern auch Gegenmaßnahmen und Referenzen zu Vorkommen der Schwachstelle in Form von CVEs. Für verschiedenste Anwendungsfälle bietet die Datenbank Mappings und Ansichten an, welche die Navigation signifikant erleichtern.

Secorvo News

Schwarze Gürtel

Im November haben Mitglieder des Secorvo-Teams drei weitere Zertifizierungen erhalten: Enes Erdoğan bestand die 24stündige Prüfung zum „Offensive Security Certified Professional" (OSCP) und ist jetzt Träger des ‚schwarzen Gürtels' für Pentester. André Domnick erwarb in einer 48stündigen Prüfung den bereits dritten DAN und darf sich nun „Offensive Security Experienced Penetration Tester" (OSEP) nennen. Und Milan Burgdorf erhielt die Zertifizierung zum ISO/IEC 27001-Auditor – die ‚Lizenz zum Prüfen'. Herzlichen Glückwunsch!

White Paper „Penetrationstests"

Viele Unternehmen führen regelmäßig technische Sicherheitsprüfungen der IT-Infrastruktur in Form von externen Penetrationstests durch. Für solche Tests haben wir aus unserer langjährigen Erfahrung eine standardisierte Vorgehensweise entwickelt, die eine wiederholbare und modularisierte Durchführung erlaubt.

Am 11.11.2021 haben wir eine überarbeitete und erweiterte Version unseres White Papers „Penetrationstests" veröffentlicht, in dem wir die Vorgehensweise von Secorvo vorstellen und konkrete Empfehlungen zur erfolgreichen Durchführung von Penetrationstests geben. Gerne finden wir auch für Sie die zu Ihrem Unternehmen passende Vorgehensweise.

Seminare

Mit sehr positiver Resonanz haben wir das Seminar „IT Security Insights" erstmals online durchgeführt: praktische Übungen und aktuelle Themen der IT-Sicherheit als ‚Update' für IT-Sicherheitsbeauftragte und -Experten. Die nächste Gelegenheit zur Teilnahme, die hoffentlich wieder in Präsenz möglich sein wird, haben Sie vom **15. bis 17.03.2022**. Davor bieten wir Ihnen vom **07. bis 11.03.2022** die Möglichkeit, sich zum T.I.S.P. zu zertifizieren, unterstützt von unserem T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz". Weitere Termine, Programme und die Möglichkeit zur Anmeldung finden Sie unter secorvo.de/seminare.

Rätseln mit Lerneffekt

Es ist wieder so weit: Mit dem interaktiven Online-Adventskalender „Krypto im Advent" lernen Schülerinnen und Schüler (3.-9. Klasse) vom 1. bis 24.12. auf spielerische Weise Verschlüsselungstechniken kennen und

können dabei attraktive Sachpreise gewinnen. Die PH Karlsruhe und die KA-IT-Si haben sich für die siebte Auflage des Adventskalenders wieder spannende Kryptografie-Rätsel ausgedacht. Ein Einstieg ist auch nach dem 1.12. noch möglich. Auch Schulklassen und Profis dürfen miträtseln, letztere allerdings außer Konkurrenz (zur kostenfreien Registrierung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2022	
14.-16.01.	ShmooCon2022 (The Shmoo Group, Washington/US)
Februar 2022	
01.-02.02.	18. Deutscher IT-Sicherheitskongress (BSI, virtuell)
03.02.	KA-IT-Si-Event „Willkommen bei den Quanten“ (KA-IT-Si, hybrid)
03.-04.02.	29. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
März 2022	
07.-11.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.-17.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, Darmstadt)
25.03.	Datenschutztag 2022 (COMPUTAS, Köln)
28.-31.03.	DFRWS EU 2022 (DFRWS, hybrid)
29.-31.03.	secIT 2022 (Heise Medien, Hannover)

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