secorvo
security consulting

Secorvo Security News

Oktober 2018

Rote Linien

Der Preikestolen ist ein Fels in der Nähe von Stavanger in Norwegen, der über 600 Meter senkrecht bis zum darunter liegenden Fjord abfällt. Hunderttausende besichtigen jährlich dieses Naturwunder. Aber keiner der Besucher, der noch bei Sinnen ist, käme auf die Idee, von dort im Wingsuit hinunter zu springen, ohne über ein gerüttelt Maß an Erfahrung als Fallschirmspringer zu verfügen.

Beim Software-Entwurf sind die roten Linien, die man tunlichst nicht überschreiten sollte, meist nicht ganz so leicht zu erkennen wie die Kante des Preikestolen. Und die möglichen Leidtragenden sind in der Regel die Anwender – und nicht die Entwickler, die die Linie überschreiten. Oft, oder besser: allzu oft verändern Designer einer Anwendung übergreifende Rechteeinstellungen des Systems, hantieren mit hoch privilegierten Benutzern und deren Credentials oder – so wie die in diesen Security News beschriebene Headset-Software – schieben dem System ein Root-Zertifikat unter, dessen Schlüssel sie gleich mit ausliefern. In solchen Fällen sollte man jedoch mindestens zweimal überlegen, ob man nicht auch ans Ziel kommt, ohne diese Linie zu überschreiten.

M M from Switzerland
(CC-BY-SA 2.0)

Wer sich dennoch in derart unsichere Gefilde begibt, der sollte beizeiten Experten für dieses Territorium hinzuziehen, die ein unabhängiges Design-Review durchführen. Zwar kann selbst dann noch etwas schief gehen – so wie leider nur zu oft auch bei Extremsportlern in Wingsuits – aber ohne eigene Erfahrung ist das Risiko unkalkulierbar und ein Scheitern wahrscheinlich.

Und noch etwas können Entwickler von Extremsportlern lernen: Hinter sich aufzuräumen und beim Gehen die Umgebung hinter der roten Linie so zurückzulassen, wie man sie vorgefunden hat.

Inhalt

secorvo
security consulting

Security News

Sennheisers HeadSetup revisited

In den SSN 08/2018 warnten wir vor dem fahrlässigen Umgang der Software Sennheiser HeadSetup mit CA-Zertifikaten. Anschließend analysierten wir einige ältere Versionen der betroffenen Software genauer – und dabei zeigte sich, dass die Schwachstelle gravierender ist als ursprünglich angenommen. Denn mit Informationen aus der Anwendung konnte auch der geheime CA-Schlüssel ausgelesen und missbraucht werden. Als „Proof of Concept" realisierten wir mit der Root-CA einen Man-in-the-Middle-Angriff auf TLS-Verbindungen und hebelten so die HTTPS-Verschlüsselung aus: Die Schwachstelle untergräbt für betroffene Systeme die gesamte zertifikatsbasierte Vertrauensinfrastruktur.

Im Gespräch mit dem Hersteller stellte sich heraus, dass die CA lediglich genutzt wird, um vertrauenswürdige Serverzertifikate für den lokal betriebenen Websocket-Dienst bereitzustellen. Dieser Dienst soll Schnittstellen zwischen Headset und Web-basierten Softphones implementieren. Dafür hätte es jedoch keiner eigenen Root-CA bedurft.

Als sei das noch nicht genug, unterliefen dem Hersteller in seinem Deinstallations- bzw. Update-Programm weitere Fehler: So werden die nicht mehr benötigten CA-Zertifikate nicht aus dem Zertifikatsspeicher von Windows entfernt. Alle Systeme, auf denen irgendwann eine der von der Schwachstelle betroffenen Versionen von HeadSetup installiert war, sind daher weiterhin angreifbar – obwohl jüngere Versionen von HeadSetup mittlerweile eine nicht so einfach zu missbrauchende CA nutzen.

Auch wenn wir die Kopfhörer des Herstellers lieben - ein Beispiel, pars pro toto, für die drastischen Folgen eines unbesonnenen Umgangs mit Credentials und Zertifikaten. Details zur Schwachstelle und Empfehlungen zu Gegenmaßnahmen finden sich in unserem Vulnerability Report zur Schwachstelle CVE-2018-17612.

Gefährliche Abhängigkeiten

Bereits am 19.01.2017 wurde über den offiziellen Twitter-Account von PHP darauf hingewiesen, dass am 31.12.2018 die Versorgung mit Sicherheits-Updates für PHP 5.6 eingestellt wird. Knapp zwei Jahre später verwenden nach den Statistiken von W3Tecs jedoch immer noch 61% aller erfassten Webseiten diese bald nicht mehr unterstützte Version. Abhilfe schafft eine rechtzeitige Migration auf eine neuere PHP-Version – die kann allerdings (zeit-)aufwändig sein.

Derartige Abhängigkeiten von Komponenten stellen vor allem im Bereich von Web-Anwendungen ein steigendes Sicherheitsrisiko dar. In der jüngsten Ausgabe der OWASP Top 10, einer Auflistung der zehn größten Sicherheitsrisiken in Web-Anwendungen, ist die Nutzung verwundbarer Komponenten erstmals in den Risiko-Katalog aufgenommen worden.

Lösungsmöglichkeiten zeigen Projekte wie RetireJS oder OWASP Dependency Check auf, die bei der Erstellung von Anwendungen bei allen Abhängigkeiten (Komponenten, Bibliotheken) prüfen, ob Versionen mit bekannten Schwachstellen verwendet werden. Das Auslaufen des Supports lässt sich allerdings noch nicht automatisiert prüfen.

Gehackte Boxen

Wer sich für die Welt der Hacks und Exploits interessiert, findet in Hackthebox eine neue Herausforderung: ein Übfeld für Hacker-Trainings. Über einen kostenlosen VPN-Zugang können Zielsysteme auf Netzwerkebene untersucht und angegriffen werden. Auch die Pentesting-Experten von Secorvo zerlegen dort regelmäßig Maschinen, testen Tools und vertiefen dabei ihre Fertigkeiten.

Der Dienst steht allen offen, die – als kleine Fingerübung – die Registrierungsseite hacken. Eine klare Empfehlung!

Abofalle „Datenschutzauskunft"

Die Schreiben der selbsternannten „Datenschutzauskunft-Zentrale" schlagen derzeit hohe Wellen in der Presse, Verbraucherschutzzentralen und Datenschützer warnen. Was ist passiert? Die in Malta ansässige „Datenschutzauskunft-Zentrale" fordert Unternehmer per Schreiben auf, sich in das Datenschutzauskunft-Register eintragen zu lassen und bietet verschiedene Dienste an. Wie bereits früher bei den so genannten „Gewerbeauskünften" steckt eine „Abofalle" dahinter: Wer das Formular ausfüllt, unterschreibt und zurücksendet schließt einen Vertrag über einen Eintrag in das Datenschutzauskunft-Register – gegen Entgelt: Es folgt eine Rechnung über mehrere hundert Euro.

Zwar gibt es bereits einstweilige Verfügungen, die der Datenschutzauskunft-Zentrale untersagen, derartige Werbung per Fax zu übersenden. Dennoch: Was tun, wenn man auf die Masche hereingefallen ist und die Betreiber mit Mahnverfahren und gerichtlicher Vollstreckung der Forderung drohen?

Nach Auffassung des Bundesgerichtshofs sind Entgeltklauseln, die derart unauffällig im Gesamtbild

eines Schreibens eingefügt sind und Dienste betreffen, die für gewöhnlich unentgeltlich erbracht werden, überraschend und damit gem. § 305c Abs. 1 BGB nicht Vertragsbestandteil, da der Vertragspartner an dieser Stelle nicht damit rechnet. Daher entsteht mit der Unterschrift keine Zahlungsverpflichtung. Allerdings gibt es bisher im Internet keine derartigen Register (warum auch), deshalb ist offen, ob die Gerichte davon ausgehen werden, dass solche Dienste in einer Vielzahl von Fällen unentgeltlich erbracht werden. Das Tätigwerden externer Datenschutzbeauftragter ist schließlich in der Regel nicht kostenlos. Allein auf das Urteil des BGH sollte man sich daher nicht verlassen, sondern den Vertrag umgehend wegen arglistiger Täuschung anfechten und rechtliche Beratung in Anspruch nehmen.

DSGVO-Abmahnungen

Vor dem Inkrafttreten der DSGVO wurde häufig eine neue „Abmahnwelle" vorhergesagt. Nun ist zu dieser Frage am 13.09.2018 eine erste Entscheidung des LG Würzburg ergangen: Ein Wettbewerber hatte die Datenschutzerklärung einer Webseite, die nicht den Anforderungen der DSGVO genügte, als wettbewerbsrechtlichen Verstoß gegen § 3a UWG abgemahnt und eine einstweilige Verfügung beantragt, die das Landgericht auch erließ.

Von einer Abmahnwelle kann bislang aber noch nicht die Rede sein, auch wenn zu erwarten ist, dass noch viele solcher Entscheidungen folgen werden. Befürchtet werden ähnliche Fallzahlen wie bei fehlerhaften oder fehlenden Widerrufsbelehrungen. Anders als bei der Widerrufserklärung gibt es hier jedoch kein gesetzliches Muster, an dem sich der Anwender orientieren könnte. Daher ist die Gefahr von Fehlern bei Datenschutzerklärungen sogar größer, wenn man nicht die notwendige Sorgfalt walten oder sich diesbezüglich beraten lässt.

Das Bundesministerium für Justiz und Verbraucherschutz hat inzwischen einen Gesetzentwurf veröffentlicht, mit dem ein weiterer Versuch unternommen wird, missbräuchlichen, auf Gewinnerzielung ausgerichteten Abmahnungen einen Riegel vorzuschieben.

Dies soll über eine Beschränkung der Klagebefugnis auf Mitbewerber und Wettbewerbsverbände erfolgen; daneben ist eine Stärkung des Schutzes von Kleinstunternehmen vorgesehen, indem ein Gegenanspruch für den Abgemahnten geschaffen wird und unangemessen hohe Vertragsstrafen keinen Anlass zur Klage begründen – sie müssen in einem angemessenen Verhältnis zum abgemahnten Verstoß und seinen wettbewerbsrechtlichen Folgen stehen, und der Streitwert darf nicht missbräuchlich hoch angesetzt werden.

Die meisten Verbände befürchten, ihre Mitglieder bzw. Verbraucherinnen und Verbraucher würden in ihrem Schutz vor Wettbewerbsverstößen beschnitten und lehnen die Einschränkung der Klagebefugnis daher ab. Begrüßt wird jedoch die Abschaffung der datenschutzrechtlichen Klagebefugnis, da für kleinere und mittlere Unternehmen ein erhöhtes Abmahnungsrisiko bestehe.

Streicht man jedoch die Klagebefugnis wegen Verstößen gegen die DSGVO aus dem Gesetz gegen den unlauteren Wettbewerb (UWG), so dürfte das den Eindruck vermitteln, dass Unternehmen es zumindest aus wettbewerbsrechtlicher Sicht mit dem Datenschutz nicht so genau nehmen müssen. So verleiht man dem Datenschutz kein größeres Gewicht, daher sollte der Gesetzentwurf sich besser darauf beschränken, missbräuchliche Abmahnungen mit Gewinnerzielungsabsicht weiter zu erschweren.

Secorvo News

Secorvo Seminare

Aktuelle Fragen der IT-Sicherheit thematisieren wir im November auf unsrem Seminar IT-Sicherheit heute (**20.–22.11.2018**). Im neuen Jahr haben Sie dann im März die nächste Gelegenheit, sich als T.I.S.P. zu qualifizieren (**25.–29.03.2019**). Wir freuen uns, Sie auf einem unserer Seminare zu begrüßen. Programme und Online-Anmeldung unter https://www.secorvo.de/seminare.

Verordnete IT-Sicherheit

Die MiRO – Mineralölraffinerie Oberrhein ist als Teil der kritischen Infrastruktur verpflichtet, die Anforderungen des § 8a IT-Sicherheitsgesetz zu erfüllen. Beim kommenden KA-IT-Si-Event am **08.11.2018** stellt Alessandro Wittig vor, wie die MiRO diese Herausforderung bewältigt hat, welche Vorteile sich daraus ergeben haben und wie der Nachweis gegenüber dem BSI erbracht wurde. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking". Wir freuen uns auf Ihre Teilnahme (Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

November 2018	
06.-07.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
14.-16.11.	42. DAFTA (GDD Gesellschaft für Datenschutz und Datensicherheit e.V., Köln)
20.-21.11.	7. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Hamburg)
20.-22.11.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
27.-28.11.	8. Handelsblatt Jahrestagung – Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
27.-30.11.	DeepSec In-Depth Security Conference Europe (DeepSec GmbH, Wien/AT)
Dezember 2018	
03.-06.12.	Black Hat Europe 2018 (Blackhat, London/UK)
2019	
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)

Fundsache

Am 11.10.2018 veröffentlichte das BSI den Bericht zur "Lage der IT-Sicherheit in Deutschland 2018". Darin finden sich – gut dargestellt – zahlreiche Beispiele aufgedeckter Angriffe und konkrete Empfehlungen zum Schutz der eigenen Infrastruktur.

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Fabian Ebner, Stefan Gora, Hans-Joachim Knobloch (Editorial), Michael Knöppler, Friederike Schellhas-Mende

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