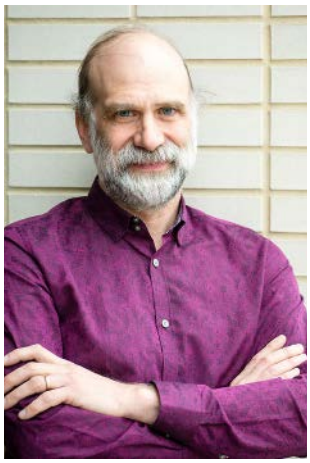
Bruce Schneier auf der SecIT 2020

Am 25. und 26. März treffen sich IT-Security-Interessierte in Hannover zum Informationsaustausch auf der secIT 2020. Im Vordergrund der Veranstaltung stehen praxisnahe Ansätze zur Bewältigung des Security-Alltags. Dazu trägt neben einer Messe mit rund 50 Ausstellern unter anderem das umfangreiche Workshop-Programm bei, bei dem die Themen Windows-10-Sicherheit, SecDevOps, Webanwendungssicherheit, KI, Notfallmanagement, Pentesting, SAP-Sicherheit und mehr vertreten sind. Eine unter anderem mit Andreas Könen, dem Abteilungsleiter „Cyber- und IT-Sicherheit" des Bundesinnenministeriums, besetzte Podiumsdiskussion greift das umstrittene Thema „Offensive Cyberverteidigung" – auch Hackback genannt – auf. Neben Verteidigungsaspekten sollen die juristische Rechtmäßigkeit sowie der praktische Nutzen oder auch Nichtnutzen beleuchtet werden.

Die durch die c't- und *iX*-Redaktion ausgewählten Vorträge informieren beispielsweise über die größte bislang in Deutschland erstellte Cybersicherheitsstudie. Befragt wurden 5000 Unternehmen, vorgestellt werden die repräsentativen Ergebnisse von Gina Wollinger, Professorin für Kriminologie und Soziologie an der Fachhochschule für öffentliche Verwaltung in Köln. TV-Computerexperte und Comedyhacker Tobias Schrödel plaudert über Dinge, die bei Stern TV nicht gezeigt werden durften. Schließlich hält Kryptopapst Bruce Schneier die Abschluss-Keynote. In seinem Vortrag „Incident Response der Zukunft" referiert Schneier darüber, wie Unternehmen sich nach einem IT-Sicherheitsvorfall am effektivsten verhalten sollten, um den Schaden so gut es geht zu begrenzen. Am Folgetag der SecIT stehen Bruce Schneier sowie die beiden deutschen Kryptoexperten und Buchautoren Klaus Schmeh und Reinhard Wobst für das Special Event „secIT Expert Lounge: Cyberwar und Schutzkonzepte" zur Verfügung. Fragen können vorab an askbruce@heise.de eingereicht werden. Das vollständige Programm sowie der Ticketshop sind über ix.de/zvsz zu finden. (ur@ix.de)



Quelle: David Betts

Gefährliche Ransomware-Varianten und -Angriffe

Um den Jahreswechsel herum analysieren Sicherheitsfirmen üblicherweise die Sicherheitsvorfälle der vergangenen 12 Monate und leiten daraus die Gefahren für das kommende Jahr ab. Einigkeit herrschte dieses Mal darüber, dass Ransomware eine der Geiseln der Zeit ist und voraussichtlich auch noch lange bleiben wird. Neue Ransomware-Varianten und -Angriffe scheinen den Experten Recht zu geben. So entdeckten Forscher der amerikanischen Sicherheitsfirma Dragos eine neue Ransomware, genannt EKANS, die außer den üblichen Verschlüsselungsfunktionen auch Schadroutinen zum Lahmlegen industrieller Steuerungsanlagen enthält (siehe ix.de/zvsz). Zwar sind die 64 Methoden, die bestimmte ICS-Prozesse außer Betrieb setzen können, derzeit noch sehr rudimentär implementiert, das wird sich jedoch mit hoher Wahrscheinlichkeit ändern, so die Forscher.

Bei der bereits 2019 entdeckten Ransomware RobbinHood konnte Sophos neue Angriffsvariationen beobachten. Dazu missbrauchen die Kriminellen legitime, digital signierte Hardwaretreiber, um vor dem Start der Dateiverschlüsselung Sicherheitsprodukte vom angegriffenen Rechner zu entfernen. Von diesem Angriff können selbst vollständig gepatchte Rechner betroffen sein, die bringen ihre eigenen Schwachstellen mit. Der signierte Treiber, der eine bekannte Schwachstelle hat, ist Teil eines veralteten Softwarepakets. Es wurde zwar vom taiwanischen Motherboard-Hersteller Gigabyte vom Markt genommen, die Software ist aber immer noch über inoffizielle Kanäle im Umlauf – auch noch gültig signiert, da weder Microsoft noch Verisign die Zertifikate widerrufen haben. So dient der Gigabyte-Treiber den Kriminellen als Türöffner, um eigene nicht signierte Treiber ins Windows-System zu laden, den Manipulationsschutz zu umgehen und Endpoint-Schutzmechanismen für den dann folgenden Ransomware-Angriff zu deaktivieren. Die Angriffsdetails beschreibt ein Sophos-Blogeintrag (ix.de/zvsz). (ur@ix.de)

Windows 10: Telemetrie deaktivierbar

Nachdem die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, kurz Datenschutzkonferenz, noch im November 2019 erklärt hatte, es sei kaum möglich, Microsofts Betriebssystem Windows 10 datenschutzkonform einzusetzen, überraschte sie nun mit der Aussage, die Übertragung der Telemetriedaten an den Softwarekonzern sei vollständig deaktivierbar. Aus dem Ende Januar 2020 veröffentlichten Tätigkeitsbericht (siehe ix.de/zvsz) des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) geht hervor, dass eine eigens gegründete Unterarbeitsgruppe der Datenschutzkonferenz namens „Windows 10" die Datenflüsse beim Einsatz des Betriebssystems unter die Lupe genommen hatte.

Unter Laborbedingungen konstatierten die Mitglieder der Arbeitsgruppe, dass sich in ihrem Testszenario – Man-in-the-Middle-Analyse bei einem Windows-10-Rechner mit installierter Enterprise-Version (Version 1909) – die Telemetriedaten komplett abschalten lassen. Nicht deaktivierbar waren lediglich Aufrufe an Microsoft-Server, die aktuelle kryptografische Zertifikate liefern. Diese sind für einen sicheren Betrieb von Windows 10 erforderlich, beispielsweise für Rückrufe eines ungültig gewordenen SSL-Wurzelzertifikats. Offen lassen die Datenschutzbeauftragten, wie der Einsatz von Windows 10 Pro zu bewerten ist, denn dort lassen sich die Telemetriedaten lediglich reduzieren, nicht abschalten. Diese Beurteilung „könnte möglicherweise ein weiterer Arbeitsauftrag der Datenschutzkonferenz (DSK) werden", so die Datenschützer. (ur@ix.de)

Kurz notiert

Seit Ende Januar gibt es am CISPA Helmholtz Center for Information Security in Saarbrücken das **French-German Center for Cybersecurity.** Es soll die Kompetenz zweier renommierter Forschungszentren für Cybersicherheit in Europa bündeln und die Forschung in diesem Bereich stärken.

Auf GitHub ist ein **von Citrix und FireEye entwickelter Scanner** für Citrix Application Delivery Controller (ADC), Gateway und SD-WAN WANOP Appliances verfügbar (ix.de/zvsz). Er überprüft, ob die Geräte über die im Dezember 2019 entdeckte Schwachstelle kompromittiert wurden.

Das Japan CERT hat die Open-Source-Software **EmoCheck zur Entdeckung der Schadsoftware Emotet** veröffentlicht (ix.de/zvsz). Dazu prüft das Tool alle laufenden Windows-Prozesse auf Auffälligkeiten, die von der Ransomware bekannt sind, und nennt die verdächtigen Dateien.