secorvo
security consulting

# Secorvo Security News

**Februar 2020**

## Von der IT lernen

Selten, dass der Mensch etwas von der Informationstechnik lernen kann. In der Regel ist es umgekehrt: Vom einfachen Algorithmus bis zur künstlichen Intelligenz versucht die IT, vom Menschen zu lernen.

Aber im Umgang mit Viren kennt sich die Informationstechnik inzwischen aus – seit dem ersten Computer-Virus aus dem Jahr 1984 sind sie eine ständige Bedrohung. Computer-Viren mutieren zudem weit schneller als Grippeviren, und die Infektionswege haben durch immer weitere Schnittstellen und die zunehmende Vernetzung der Systeme ständig zugenommen. Trotzdem ist bis heute ein „GAU“ ausgeblieben.

Das Erfolgskonzept der Virenabwehr in der Informationstechnik ist die Reaktion auf verschiedenen Ebenen. Am einfachsten lässt es sich in fünf Schritten beschreiben:

1. Expertenanalyse des Virus direkt nach erstem Auftreten
2. Unverzügliche und umfassende Information über Infektionswege, Schad-Funktion und wirksame erste Gegenmaßnahmen
3. Sensibilisierung der Nutzer für Symptome und Infektionswege
4. Blockade einzelner Infektionswege (z. B. durch Updates)
5. Isolation befallener Systeme

Tatsächlich eignen sich nicht alle Maßnahmen, die gegen Computerviren helfen, auch für Menschen, wie das Neuaufsetzen des Betriebssystems oder das Formatieren der Festplatte.

Allerdings gilt auch für „echte“ Viren: Keine Panik. Ausbreitung und Schäden lassen sich eindämmen. Ruhe bewahren – aber zugleich alle riskanten Tätigkeiten vermeiden. Und immer wieder gründlich die Hände scannen – pardon: waschen.

## Inhalt

# Security News

## Gemeinsam verantwortlich

Bereits im Datenschutz-Tätigkeitsbericht 2019 legte der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI), Dr. Stefan Brink dar, dass angesichts der aktuellen Rechtslage insbesondere im Bereich Social Media Unklarheiten bei der Gemeinsamen Verantwortlichkeit bestehen. Am 06.02.2020 informierte der LfDI via Pressemitteilung über einen für öffentliche Stellen erstellten Anforderungskatalog der Aufsichtsbehörde. Danach riskiert die einen solchen Dienst einsetzende verantwortliche Stelle von der Aufsichtsbehörde in die Pflicht genommen zu werden, wenn die Anforderungen nach Art. 26 DSGVO vom Plattformbetreiber nicht angeboten und auch auf Anforderung des Nutzers nicht umgesetzt werden.

Der Anforderungskatalog sollte auch von Unternehmen geprüft werden, da die Anforderungen der Aufsichtsbehörde übertragbar sind. Wer in einem solchen Fall auf die Nutzung von Social-Media-Diensten nicht verzichtet, muss sich darüber im Klaren sein, dass er damit das Risiko eines Bußgeld bewehrten DSGVO-Verstoßes in Kauf nimmt.

## Audit? Aber sicher!

Wie wichtig es ist, bei Security-Audits auf Qualität zu achten, haben im Februar die Audits zweier Wahl-Apps aus den USA gezeigt. So legte ein von Pro Publica in Auftrag gegebenes Security-Audit offen, dass die bei den Vorwahlen in Iowa verwendete Wahl-App von „elementaren Sicherheitsproblemen" betroffen ist, über die u. a. eine Manipulation der Anzahl der Stimmen möglich gewesen wäre. Der Hersteller behauptet, die App wäre zuvor „mehreren rigorosen Sicherheitstests durch eine Drittpartei" unterzogen worden. Auch die bereits mehrfach in den USA eingesetzte Wahl-App „Voatz" hat erhebliche Sicherheitsmängel, wie Forscher des MIT am 13.02.2020 mitteilten. Die Schwachstellen erlauben einem Angreifer Stimmen zu manipulieren, Stimmabgaben zu unterdrücken oder zu erkennen, für wen ein Wähler gestimmt hat. Auch für Voatz gab es laut Hersteller in der Vergangenheit diverse Sicherheitsaudits.

Security-Audits sollte man grundsätzlich von qualifizierten, idealerweise auch zertifizierten Auditoren nach anerkannten Prüfstandards durchführen lassen. Damit werden die Ergebnisse vergleichbar – und Vorfälle wie die oben genannten sollten seltene Ausnahmen sein.

## Keep it simple

Am 28.01.2020 hat Linus Torvalds WireGuard in den Hauptzweig des Linux-Kernels aufgenommen. WireGuard realisiert ein neuartiges VPN-Protokoll, das einfacher, sicherer und performanter sein will als die VPN-Standards OpenVPN und IPsec.

Mit nur etwa 4.000 Zeilen Quellcode (loc) ist die Komplexität von WireGuard deutlich geringer als die von OpenVPN und OpenSSL (70.000 bis 600.000 loc) oder IPSec (400.000 loc). Damit sinkt die Fehleranfälligkeit und das Auditieren des Quelltextes wird erheblich erleichtert. Durch die Beschränkung auf das absolute Minimum – beispielsweise wird nur eine einzige Cipher Suite unterstützt und statt X.509-Zertifikaten kommen wie bei SSH Schlüsselpaare zum Einsatz – bietet WireGuard nicht denselben Funktionsumfang wie OpenVPN; das könnte eine Hürde bei der Durchsetzung sein. Aus Sicherheitssicht ist WireGuard jedoch ein Schritt in die richtige Richtung – denn Komplexität ist einer der großen Feinde der IT-Sicherheit.

## Erpressung „on top"

Dass man Ransomware für die Betroffenen noch unangenehmer gestalten kann, haben die Macher der „MAZE"-Ransomware um den 05. und 09.12.2019 unter Beweis gestellt. Dafür kombinierten sie zwei schon lange von Cyberkriminellen genutzte „Geschäftsmodelle", um den Zahlungsdruck zu erhöhen: Zunächst werden die Daten gestohlen und wie üblich verschlüsselt. Kommt der Betroffene der Zahlungsaufforderung nicht nach, werden die gestohlenen Daten in kleinen Häppchen im Internet veröffentlicht. Besonders verheerend kann das angesichts hoher DSGVO-Bußgelder sowohl für Unternehmen als auch für Privatpersonen sein.

Wer bereits Maßnahmen zum Schutz vor Ransomware (SSN 02/2016 und SSN 04/2016) ergriffen hat und eine solide, getestete Disaster-Recovery-Strategie mit Backups umsetzt, sollte sich daher besser nicht zufrieden zurücklehnen und das Thema „Data Loss Prevention" aus den Augen verlieren...

## IT-Grundschutz 2020

Das BSI hat – wie geplant – am 01.02.2020 die 2020er Edition des IT-Grundschutz-Kompendiums veröffentlicht. Mit der Umstellung der IT-Grundschutz-Kataloge auf das IT-Grundschutz-Kompendium verfolgte das BSI das Ziel, die Aufwände für die Konzepterstellung zu reduzieren und die Praktikabilität bei der Umsetzung zu erhöhen (SSN 8/2018) – aus der Praxis können wir bestätigen, dass das gelungen ist.

Neu in der Edition 2020 sind die Bausteine „CON.8 Software-Entwicklung" sowie „NF.5 Raum sowie

Schrank für technische Infrastruktur"; die weiteren Änderungen sind klar aufgeführt. Alte Zöpfe, wie die Anforderung, regelmäßig das Kennwort zu wechseln – „Die Passwörter SOLLTEN in angemessenen Zeitabständen geändert werden." (ORP.4.A8) – wurden bei der Gelegenheit auch abgeschnitten. Aus unserer Sicht ist die neue Fassung eine weitere Verbesserung dieses wichtigen Referenzwerkes der IT-Sicherheit.

### Conditio sine qua non

In der Automobilbranche sind Anforderungen an die IT-Sicherheit wie eine TISAX-Zertifizierung mittlerweile Standard. Andere Branchen ziehen nach: So wurde in einer europaweiten Ausschreibung im Bereich Krankenkassen/Sozialdienste (Unterstützungsdienstleistungen Fallbearbeitung) von den Bietern ein ISMS-Zertifikat nach DIN EN ISO 27001 gefordert. Eine Bietergemeinschaft wurde ausgeschlossen, obwohl eines der Mitglieder zertifiziert war. Daraufhin hatte ein anderes, nicht zertifiziertes Mitglied den Ausschluss vor dem Bundeskartellamt angegriffen. Dieses wies den Nachprüfungsantrag jedoch bereits am 19.07.2019 zurück.

Das Beispiel zeigt, dass nach einer langen Phase der Zurückhaltung inzwischen auch in Deutschland ein ISMS zunehmend zum Stand der Technik gezählt und von Anbietern erwartet wird.

### Mixed Content

Am 06.02.2020 kündigte Joe DeBlasio vom Chrome Security Team im Google Security Blog an, dass Chrome zukünftig Schritt für Schritt Mixed-Content-Downloads verhindern wird. Damit werden von verschlüsselten Seiten keine unverschlüsselten Downloads mehr möglich sein. Dies setzt die Ende 2019 angekündigten Bestrebung fort, Mixed Content in Chrome komplett zu blockieren. Dass dieses Vorgehen bei Herstellern problematische Umgehungsstrategien provozieren kann, hat 2018 der Sennheiser-Fall gezeigt (SSN 11/2018).

Entwickler sollten dennoch prüfen, ob ihre Anwendungen Mixed-Content-Downloads durchführen und diese auf HTTPS umstellen. In der Praxis beobachten wir insbesondere in Unternehmensnetzen noch vergleichsweise oft unverschlüsselte Kommunikation. Da diese in aktuellen Browsern zukünftig weiteren Beschränkungen unterliegen wird, erscheint auch hier der Umstieg auf HTTPS angebracht.

## Secorvo News

### Secorvo Seminare

Wenige Tage noch bis zum „TeleTrusT Professional for Secure Software Engineering" – einem interaktiven Seminar mit großem Praxisteil zur sicheren Softwareentwicklung (**16.–19.03.2020**). Und im Mai folgt das nächste T.I.S.P.-Seminar (**11.–15.05.2020**) – wer bereits jetzt mit der Vorbereitung anhand des jüngst aktualisierten Begleitbuchs zum T.I.S.P. beginnen möchte, sollte sich einfach anmelden – das Begleitbuch wird Ihnen umgehend zugesendet (Programme und Online-Anmeldung).

### EaSy mit Microsoft-PKI

Unsere Zertifikatsmanagement-Lösung Certificates ready2go – EaSy erhält im nächsten Release (April 2020) die Möglichkeit zur Anbindung einer Active Directory Enterprise CA. Über das EaSy Enrollment-Gateway können ACME Clients wie der bekannte Certbot für interne Server öffentlich gültige Zertifikate bei Trustcentern wie Let's Encrypt & Co. beziehen und automatisch erneuern – und künftig auch intern gültige Zertifikate bei einer vorhandenen Microsoft-PKI. Für die internen Zertifikate entfällt die Beschränkung auf öffentlich registrierte Servernamen; die Enterprise CA kann Zertifikate auch für bspw. „intranet.local" erstellen (Kontakt).

### „Ich seh' etwas, was Du nicht siehst…"

Das kommende KA-IT-Si-Event am 26.03.2020 dreht sich um die Sichtbarmachung des Unsichtbaren: Die Sicherheit eines Verfahrens oder Protokolls kann man nämlich nicht durch einfaches Hinsehen erkennen, wie Professor Dr. Jörn Müller-Quade (KIT) zeigen wird. Schlimmer noch: Sie ist keine funktionale Eigenschaft und kann daher auch nicht durch einfaches Testen festgestellt werden.

Dem begegnet die Kryptographie mit mathematischen Beweisen, mit denen nachgewiesen wird, dass ein Verfahren in einem bestimmten Modell unter präzise beschriebenen Voraussetzungen eine ebenso präzise definierte Sicherheitseigenschaft erfüllt. Unterschiede zwischen dem (vereinfachenden) Modell und der Wirklichkeit können dazu führen, dass auf die Implementierung eines als sicher bewiesenen Systems so genannte Seitenkanalangriffe möglich sind. Noch gravierender ist, dass nicht ohne weiteres nachprüfbar ist, ob ein reales technisches System auch wirklich die modellierte Sicherheitslösung umsetzt. Ein Ansatz, diesem Problem zu begegnen, ist *Auditable Security* – ein Konzept, das durch den modularen Aufbau von Systemen eine Überprüfung bestimmter Eigenschaften durch eingehende visuelle Inspektion zu ermöglichen versucht.

Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

## Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

| | |
|---|---|
| **März 2020** | |
| 16.-19.03. | T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe) |
| 17.-20.03. | GI Sicherheit 2020 (Gesellschaft für Informatik e.V., Göttingen) |
| 25.-26.03. | secIT 2020 (Heise Medien, Hannover) |
| 25.-27.03. | DFRWS EU Conference (DFRWS, Oxford/UK) |
| 31.03.-03.04. | Blackhat Asia 2020 (Blackhat, Singapur/SIN) |
| **April 2020** | |
| 21.-22.04. | Datenschutztage 2020 (FFD, Wiesbaden) |
| 21.-22.04. | Security Forum 2020 (Hagenberger Kreis, Hagenberg/AT) |
| **Mai 2020** | |
| 06.-07.05. | BvD Verbandstag 2020 (BvD e.V., Berlin) |
| 10.-14.05. | Eurocrypt 2020 (IACR, Zagreb/HRV) |
| 11.-15.05. | T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe) |
| 12.-15.05. | European Identity & Cloud Conference 2020 (KuppingerCole Ltd., München) |


## Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: André Domnick, Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Sarah Niederer, Friederike Schellhas-Mende, 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