Sicher wie die TI-tanic

Hinweise auf mögliche Verwundbarkeiten der Medizin-Telematik

Weil sich Zugangskarten rund um die Telematik-Infrastruktur (TI) für Ärzte, Kliniken und Kassen ohne Identitätsprüfung besorgen ließen, stoppte die gematik vorerst die Ausgabe. Eine Analyse des Sicherheitsexperten Thomas Maus legt die Vermutung nahe, dass es um die technische Seite nicht besser steht.

Von Thomas Maus

Gesundheitsminister Jens Spahn hatte wohl keinen ruhigen Jahreswechsel. Denn zwischen den Feiertagen zeigte Sicherheitsexperte Martin Tschirsich zusammen mit Dr. Christian Brodowski und Dr. André Zilch auf dem Kongress des Chaos Computer Clubs in Leipzig, wie einfach jedermann an Zugangskarten und -hardware der Telematik-Infrastruktur (TI) für Ärzte und Praxen sowie an fremde elektronische Gesundheitskarten (eGK) gelangen konnte – ohne sich ausweisen zu müssen. Dazu waren keinerlei Hacks nötig, sondern lediglich ein paar frei zugängliche Informationen einer Praxis und eines Arztes, schon konnten sie sich Karten und Komponenten zu einer geänderten Adresse bestellen (siehe ct.de/y4tz).

Die gematik, die die Vernetzung der Praxen durch die TI vorantreibt, reagierte prompt und sperrte die Produktion und Ausgabe aller Praxis- und Heilberufs-Ausweise. Zusammen mit allen Kartenanbietern erarbeitet sie neue Vorgaben für die Identitätsfeststellung der Empfänger. Eine Sprecherin des Anbieters medisign hoffte, dass der Ausgabestopp Mitte Januar aufgehoben werde. Unter anderem werde es fortan keine Auslieferung an alternative Adressen mehr geben. Tschirsich, Brodowski und Zilch hatten die Untauglichkeit der Verfahren KammerIdent und BankIdent zur Identitätsfeststellung eines Arztes nachgewiesen, sie würden deshalb ausgesetzt – einzig das PostIdent-Verfahren solle übrig bleiben. „Es ist davon auszugehen, dass es künftig strengere Restriktionen für die Auslieferung geben wird, die den Komfort einschränken und den Aufwand für die Beschaffung erhöhen“, erklärte medisign gegenüber c’t.

Laut Martin Tschirsich sind derzeit rund 115.000 von 170.000 Arztpraxen in Deutschland an die TI angeschlossen. Praxen ohne Anschluss werden mit Honorarabzügen von derzeit ein Prozent bestraft. Ob auch diese Abzüge ausgesetzt werden, solange sich neue Ärzte und Praxen mangels Zugangskarten nicht mit der TI verbinden können, konnte uns die Kassenärztliche Bundesvereinigung auf Nachfrage nicht beantworten. Die Entscheidung läge bei den einzelnen Kassenärztlichen Vereinigungen.

Die als fälschungssicher geltenden elektronischen Ausweise für Ärzte und Praxen konnte sich bislang also jeder an irgendeine Käsetheke liefern lassen. Für die Bestellung einer fremden Gesundheitskarte genügte eine simple E-Mail an die Krankenkasse. Da auf den eGKs unter anderem auch Informationen zur Teilnahme an Chroniker-Programmen gespeichert sind, können Betrüger hier durchaus sensible Gesundheitsdaten abgreifen. Zumindest bei den eGKs ist das Problem seit 2004 bekannt – da ist es völlig unverständlich, warum die Datenschutzbeauftragten der Länder und des Bundes noch kein Auge darauf geworfen haben.

Freie Bahn für Emotet

Doch selbst wenn gematik und Bundesgesundheitsministerium die Identifizierung von Ärzten, Praxen und Patienten bei der Kartenausgabe künftig verbessern, könnten in der TI womöglich noch hunderte weitere Sicherheitslücken klaffen. Um diesen auf die Spur zu kommen, hat der Autor als Sicherheitsexperte im Auftrag von Ärzten an deren Konnektoren nichtinvasive und nichtdestruktive Analysen durchgeführt. Diese beschäftigen sich ausführlich mit dem Modell von T-Systems, das neben dem KoCoBox-Konnektor von CGM (dazu später mehr) in Praxen am weitesten verbreitet ist. Konnektoren verbinden Arztpraxen per VPN mit der Telematik-Infra-

struktur und bilden damit das Herzstück für deren Sicherheitsarchitektur.

In der TI sollen künftig mit Einführung der elektronischen Patientenakte (ePA) ab Anfang 2021 nicht nur die Gesundheitsdaten von 73 Millionen Patienten in Deutschland zentral verwaltet und ausgetauscht werden. Die TI soll darüber hinaus auch zur sicheren Kommunikation der Praxen und Kliniken untereinander dienen.

Bislang predigen gematik und Gesundheitsministerium, dass die TI mit ihren Konnektoren und Kartenterminals „optimal sicher“ sei. Probleme entstünden allein durch Nachlässigkeiten von Ärzten und deren IT-Dienstleistern, wenn sie veraltete Software nutzten und das LAN der Praxis nicht richtig absicherten.

Diese „Nachlässigkeiten“ sind jedoch eher die Regel als die Ausnahme. Laut Recherchen des NDR wurde beispielweise die von der gematik favorisierte serielle Installationen des Konnektors nur in zehn Prozent der Praxen umgesetzt. In dieser Konfiguration ist der Konnektor die einzige Verbindung der Praxis zur Außenwelt: Er baut nicht nur das VPN zur Telematik-Infrastruktur auf, sondern dient gleichzeitig als Firewall für das Praxis-LAN Richtung Internet. Von den übrigen Praxen mit paralleler Konfiguration, bei der die Praxis ihre Internet-Verbindung in Alleinregie absichern muss, befänden sich rund ein Drittel in einem desolaten Sicherheitszustand.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiß das: „... muss nach dem Stand der Technik davon ausgegangen werden, dass Leistungserbringer eine Kompromittierung eines ihrer IT-Systeme im LAN nicht sicher verhindern bzw. nicht in jedem Fall frühzeitig erkennen können.“ (Konnektor-Schutzprofil BSI-CC-PP-0047-2015-MA-01, Abschnitt 7.6.2). Trotzdem setzt dasselbe Schutzprofil ein unkompromittiertes Praxis-LAN für die Sicherheit der TI voraus.

Hier liegt ein offenkundiger Widerspruch und ein fundamentaler Design-Fehler in der Sicherheitsarchitektur: Eine einzige kompromittierte Praxis stellt die Sicherheit vieler ePAs in Frage. Das angeblich „geschlossene medizinische Netz“, welches ein „Höchstmaß an Schutz“ bieten soll, ist dann eben nicht mehr geschlossen.

Wird ein Konnektor oder ein anderer Teil der TI kompromittiert, dann lassen sich womöglich nicht nur Gesundheitsdaten abgreifen und manipulieren. Angreifer könnten über in der ePA abgelegte Dokumente (darunter PDFs) auch Viren und Trojaner einspielen. Es bestünde dann Gefahr, dass sich Emotet-Angriffe, wie sie jüngst Kliniken in Fürth und Hannover lahmlegten, über die TI auf andere Praxen und Krankenhäuser ausbreiten – und das auf höchstem Sicherheitsniveau.

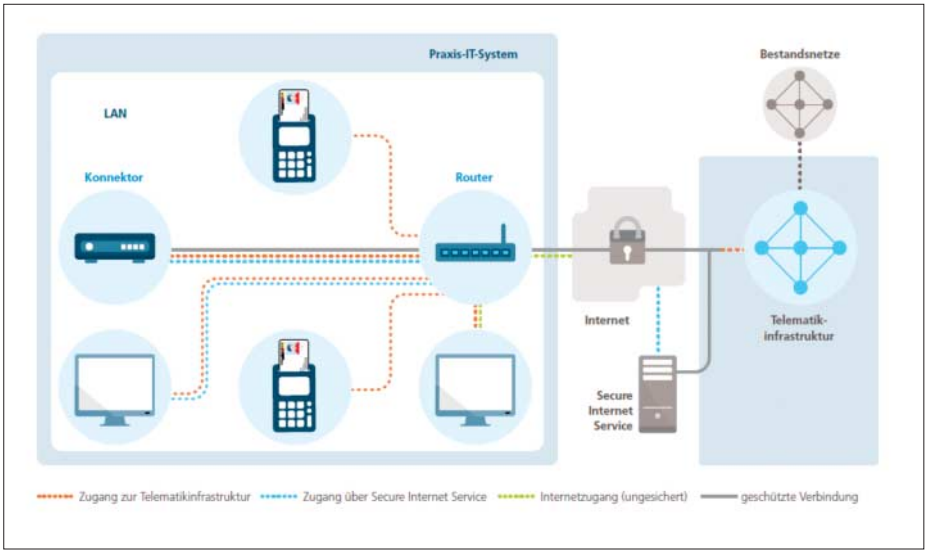

Bild: gematik vom 28.8.2019

90 Prozent der Praxen nutzen eine parallele Installation des Konnektors für die TI, bei der das übrige Praxis-LAN von einem separaten Router abgesichert wird.

Zertifikatsfehler

Doch selbst bei einer seriellen Konnektor-Konfiguration ist nicht alles in Butter: Der Konnektor fungiert dann nämlich gleichzeitig als Firewall für das Praxis-LAN und ist somit angriffsexponiert und sicherheitskritisch.

Diesem Anspruch wird der „Medical Access Port“ genannte Konnektor von T-Systems womöglich nicht gerecht. Der Konnektor wird über ein Web-Frontend konfiguriert. Der Browser des Admin ruft bei der ersten Verbindung ein Zertifikat vom Konnektor ab, das für eine verschlüsselte Verbindung (HTTPS) benötigt wird. Beim T-Systems-Konnektor produziert die Echtheitsprüfung im Browser jedoch einen Zertifikatsfehler. In allen untersuchten Praxen hatten die IT-Dienstleister (DvOs) den Ärzten geraten, die Warnung „einfach wegzuklicken“.

Diese Ignoranz führt das Konnektor-Zertifikat jedoch ad absurdum und öffnet Man-in-the-Middle-Angriffen Tür und Tor, die das Admin-Passwort abgreifen. Angreifer in Gestalt von Patienten, Reinigungspersonal oder Lieferanten bräuchten dazu lediglich ein Gerät für unter 100 Euro im Praxis-LAN zu platzieren, und schon könnten sie Kontrolle über den Konnektor erlangen. Dagegen kann sich eine Arztpraxis mit typischer IT-Ausstattung und -Personal kaum schützen.

Open-Source-Komponenten

Zurück zum Konnektor: Das System basiert in großem Umfang auf Open-Source-Komponenten und würdigt dies entsprechend der Lizenzbestimmungen durch deren Benennung. Die auf der Admin-Oberfläche des Konnektors einsehbare Liste (siehe ct.de/y4tz) erstreckt sich über 77 Einträge und wirft sofort Fragen auf. Denn auf sicherheitskritischen Systemen sollten niemals mehr Komponenten installiert sein als unbedingt nötig, weil sie die Angriffsfläche unnötig vergrößern.

Auf dem Konnektor ist jedoch unter anderem ein WPA-Supplicant installiert, der lediglich für WLANs relevant wäre. Ebenso findet sich die E-Mail-Library mimetic, obwohl der Konnektor gar keine Mails verschickt – zumindest offiziell.

Bedenklich ist das hohe Alter einiger Komponenten: Eine xqc-Version (wahrscheinlich eine C-Schnittstelle zur XML-Query-Language) stammt offenbar vom Mai 2013, jQuery (eine populäre Bibliothek für JavaScript) vom Mai 2014.

Eine Reihe von Paketen aus dem Node.js- beziehungsweise NPM-Universum erstaunt ebenfalls auf einem sicherheitskritischen Gerät, denn die Sicherheitshistorie von NPM ist ziemlich unrühmlich.

Schließlich ist sogar der Paketmanager opkg dabei. Er dient dazu, Software-Pakete auf dem neuesten Stand zu halten. Auf sicherheitskritischen Geräten wie

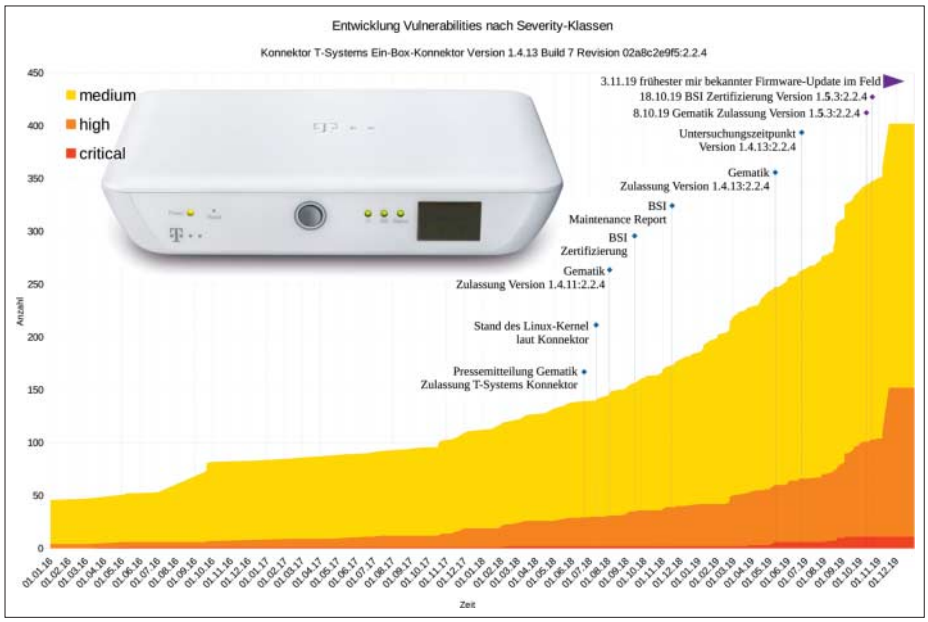

Bild: Thomas Maus

Die Grafik zeigt das Ansteigen der bekannt gewordenen Sicherheitslücken der Open-Source-Komponenten, die auch beim TI-Konnektor von T-Systems (Firmware 1.4.12, Hardware-Revision 2.2.4) zum Einsatz kommen.

einem Konnektor dürfen aber auf gar keinen Fall irgendwelche Updates aus ungesicherten Quellen aufgespielt werden. Jedes einzelne Update muss zuvor aufwendig geprüft und zertifiziert werden. Deshalb erscheinen offizielle Firmware-Updates des Konnektors auch nur einmal im Jahr. Denn die nötige Zertifizierung nach dem internationalen Common-Criteria-Standard beschäftigt mehrere Sicherheitsprüfer über Wochen und kostet sechsstellige Beträge. Dynamische Updates wären zertifizierungswidrig.

Die TI ist sicher …

Um einzuschätzen, wie verwundbar die auf dem Konnektor eingesetzte Software ist, hat der Autor zu allen Komponenten die bekannten Verwundbarkeiten herausgesucht. Diese werden in der CVE-Datenbank (Common Vulnerability Enumeration) gesammelt. Theoretisch müssten in jedem CVE-Eintrag auch die betroffenen CPE (Common Product Enumeration) aufgeführt sein. Praktisch fehlen die CPEs teils ganz oder es wird nur im Freitext erwähnt, dass die Verwundbarkeit auch in allen früheren Versionen besteht – was den Aufwand erheblich vergrößert.

Die im Konnektor von T-Systems eingesetzte Software (Firmware 1.4.13) lieferte bei einem Abgleich mit der CVEsearch-Datenbank vom 31.12.2019 sage und schreibe 3335 Treffer. Beschränkt man die Suche auf die exakten CPE-Einträge, passen immer noch 1043 Einträge, auf die sich die weitere Analyse konzentriert.

Die Brisanz der Verwundbarkeiten wird nach dem CVSS (Common Vulnerability Scoring System) eingestuft. Die Skala reicht von 0 bis 10: Low (unter 4), Medium (4 bis unter 7), High (7 bis unter 9) und Critical (9 bis 10). Soweit Security-Patch-Backports plausibel zu vermuten waren – etwas beim Kernel –, wurden die entsprechenden CVEs ignoriert.

Filtert man noch alle Low-Einstufungen heraus (worüber man streiten kann), so verbleiben im T-Systems-Konnektor (Firmware 1.4.13) Hinweise auf mindestens 402 potenzielle Verwundbarkeiten: 11 kritische, 141 hochbrisante, 250 mittelbrisante (Stand 31.12.2019).

Nicht viel besser sieht es nach dem Firmware-Update aus, das T-Systems während des Untersuchungszeitraums am 28. November 2019 veröffentlichte. Die neue Firmware-Version 1.5.3 hatte am 31. Dezember immer noch 291 Hinweise auf klärungsbedürftige Verwundbarkeiten: 7 kritische, 117 hochbrisante und 167 mittelschwere.

Dieser Wert ist aber keine Konstante – er entwickelt sich über die Zeit. Deshalb stellt sich die Frage, welche dieser Verwundbarkeiten bereits während der Zertifizierung bekannt waren, und von T-Systems eventuell manuell hätten gepatcht werden können, und welche erst später hinzukamen. In der Grafik links haben wir deshalb den zeitlichen Verlauf aufgetragen, mit dem die Zahl der Verwundbarkeiten im Konnektor anstieg.

… ein Problem

Neben der bloßen Anzahl der Verwundbarkeiten alarmiert auch die Schwere einiger besonders kritischer Sicherheitslücken im CVE-Abgleich mit den Komponenten des Konnektors: Das fängt mit Anfälligkeiten für Denial-of-Service-Attacken an (CVE-2018-5391, CVE-2019-11477 und CVE-2018-5388), geht über Man-In-the-Middle-Attacken bei der Kernfunktion des VPN, weil sich die Authentifikation mit RSA bei IKEv2 unterlaufen lässt (CVE-2018-16151 und CVE-2018-16152), bis hin zu zahlreichen möglichen Pufferüberläufen, die nicht selten darin münden, dass ein Angreifer beliebigen Code ausführen kann (zum Beispiel CVE-2018-17540, CVE-2016-2108, CVE-2015-0292). Allein die in der Liste auftauchende sicherheitskritische, uralte OpenSSL-Version 0.9.8w besitzt eine kritische und fünf hochbrisante Verwundbarkeiten.

Neben dem Konnektor ist auch das Kartenterminal sicherheitskritisch. Nicht umsonst kleben auf dem Gehäuse diverse Sicherheitssiegel des BSI, die ein unbemerktes Öffnen verhindern sollen. Ein solches Terminal ist über das Praxis-LAN mit dem Konnektor verbunden und wacht über die Verwendung der digitalen Patienten- und Arzt-Identitäten sowie über den Zugriff auf Patientendaten.

In der Grafik auf Seite 17 sind analog zum T-Systems-Konnektor mögliche Verwundbarkeiten des derzeit am weitesten verbreiteten Kartenterminals Ingenico ORGA 6141 online im zeitlichen Verlauf aufgezeichnet. Mit über hundert mittleren bis hohen sowie weiteren kritischen CVE-Einträgen, die sich seit der letzten Aktualisierung eingeschlichen haben, ist es zweifelhaft, dass das Kartenterminal ein „europaweit einzigartiges Sicherheitsniveau“ erreicht, von dem Gesundheitsministerium und gematik schwärmen.

Natürlich führt nicht jede in der CVE-Datenbank aufgeführte Verwundbarkeit zu einem tatsächlich durchführbaren Angriff. Doch für jede Verwundbarkeit, die zum Zeitpunkt der Zertifizierung bekannt ist, müsste mindestens dokumentiert sein, warum sie die Sicherheit des Systems nicht schwächen kann. Dazu dient die in der Zertifizierung vorgesehene AVA_VAN (Activity Vulnerability Assessment – Vulnerability ANalysis). Für die aufgelisteten

CVE-Einträge des Konnektors und Kartenterminals existieren jedoch keine öffentlichen Dokumentationen, die deren Unbedenklichkeit nachweisen.

Oldtimer Common Criteria

Das in den 90er-Jahren entstandene Zertifizierungssystem „Common Criteria“ (CC) – nach dem Konnektoren und Kartenterminals zertifiziert werden – ging noch davon aus, das Software entweder korrekt oder aber defekt ist. Heutzutage ist diese Vorstellung jedoch überholt. Eine Komponente kann zum Zeitpunkt der Zertifizierung sicher sein, weil noch niemand einen Angriffsweg entdeckt hat. Wenn ein solcher Weg aber später publik wird, ist die Komponente fortan nicht mehr sicher. Im Fall eines Konnektors müsste er so lange abgeschaltet werden, bis die Unbedenklichkeit bewiesen oder die anfällige Komponente erneuert und der Angriffsweg versperrt ist. Dann könnte der Konnektor wieder weiterlaufen – bis zur Entdeckung einer neuen Verwundbarkeit.

Das Problem ist die statische Vorstellung von Programmcode in der CC-Welt, seiner Korrektheit und Sicherheit. Dies sieht man an den CC-Maintenance-Reports: Das Gerät wird als unverändert betrachtet, weswegen keine erneute Zertifizierung notwendig ist. Das Gerät mag unverändert sein, aber das Wissen über seine Sicherheitseigenschaften hat sich teils dramatisch verändert, wie die Grafiken zeigen.

Das ist keine Kritik am Einsatz von Open-Source-Software. Tatsächlich ist er eine gute Idee, wenn durch koordinierte Sichtungen der Quellen Verwundbarkeiten systematisch beseitigt würden. Jede CVE ist ja eine bekannte Schwachstelle, die meistens wenige Tage nach Bekanntwerden durch ein Update aus dem Verkehr gezogen wird. Von der Qualitätssicherung der CVEs kann man jedoch nur profitieren, wenn man Updates in hoher Frequenz durchführt – und dies ist innerhalb der Common Criteria kaum sinnvoll möglich.

Geheimnis der KoCoBox

Nun wäre es jedoch kurz gedacht, wenn man der Telekom die Nennung der im T-Systems-Konnektor verwendeten Open-Source-Komponenten ankreiden würde. Konkurrent CGM bedient sich für seine KoCoBox MED+ ebenfalls bei Open-Source-Code. Der Hersteller listet jedoch lediglich die Lizenzen, aber nicht die Komponenten auf und verstößt somit zumindest gegen die GNU General Public License. Wenn CGM die verwendeten Open-Source-Komponenten nicht angibt, muss man für die KoCoBox vom schlimmsten Fall ausgehen, also allen Verwundbarkeiten jeglicher Software unter all den angegebenen Lizenzen.

Updaten? Abschalten!

Ärzte, die den Konnektor von T-Systems einsetzen, sollten dessen Firmware – falls noch nicht geschehen – unbedingt von Version 1.4.13 auf die Ende November veröffentlichte Version 1.5.3 updaten. Dadurch können sie immerhin die Zahl der möglichen klärungsbedürftigen Verwundbarkeiten von 402 auf 291 senken. Das ist besser, aber noch lange nicht gut. Deshalb kann der Autor selbst bei einem aktualisierten Konnektor Ärzten nur raten: abschalten.

Das ist keine pauschale Warnung vor der Digitalisierung der Medizin, sondern vor einer ungesicherten Vernetzung durch die TI. Würden Praxen und Kliniken alle digitalen Systeme mit veralteter Software abschalten, stünden Ärzte weitgehend ohne moderne Diagnostik da. Isoliert oder in Inselnetzen erzeugen aber selbst die immer noch anzutreffenden Windows-XP-Rechner zur Steuerung von Röntgengeräten kaum Gefahr – aber erheblichen Nutzen.

Aber selbst wenn die gematik zusichert, dass alle CVEs der Konnektoren und Kartenterminals einzeln geprüft wurden und tatsächlich keine Gefahr besteht, hilft das nur, bis die nächste Verwundbarkeit bekannt wird. Deren Prüfung dauert dann wieder einige Tage, in denen die Sicherheitslage unklar ist. Bei höchstem Sicherheitsniveau, das für Medizin-IT und Gesundheitsdaten gefordert wird, ist dies nicht akzeptabel: Die Konnektoren müsste man derweil abschalten.

Obige Analyse deckt allerdings nur einen kleinen Teil möglicher Probleme der Telematik-Infrastruktur auf: Ob Zertifizierungsniveau oder -verfahren, Installationsqualität, Management der Authentifikationsmittel oder Updates – wo immer unabhängige Experten bisher im Rollout der TI hinschauten, blickten sie in Abgründe. So ließen sich bislang nicht einmal unabhängige Penetrationstests durchführen, weil die gematik die dazu nötigen Sandbox-Systeme nicht zur Verfügung stellt.

Das enorme Tempo, mit dem das Gesundheitsministerium unter der Leitung von Jens Spahn – Zitat: „Ich werde bei dem Thema gematik mehr Geschwindigkeit reinbringen, Hacker hin oder her.“ – den Ausbau der TI trotz aller Bedenken vorantreibt, erinnert an den euphorischen Fortschrittsglauben im viktorianischen Zeitalter. Damals hielt man die Titanic für unsinkbar und steuerte mit ihr trotz aller Warnungen unter Volldampf voraus – in den nächsten Eisberg. *(hag@ct.de)* c't

CCC-Vortrag und Open-Source-Listen:
ct.de/y4tz

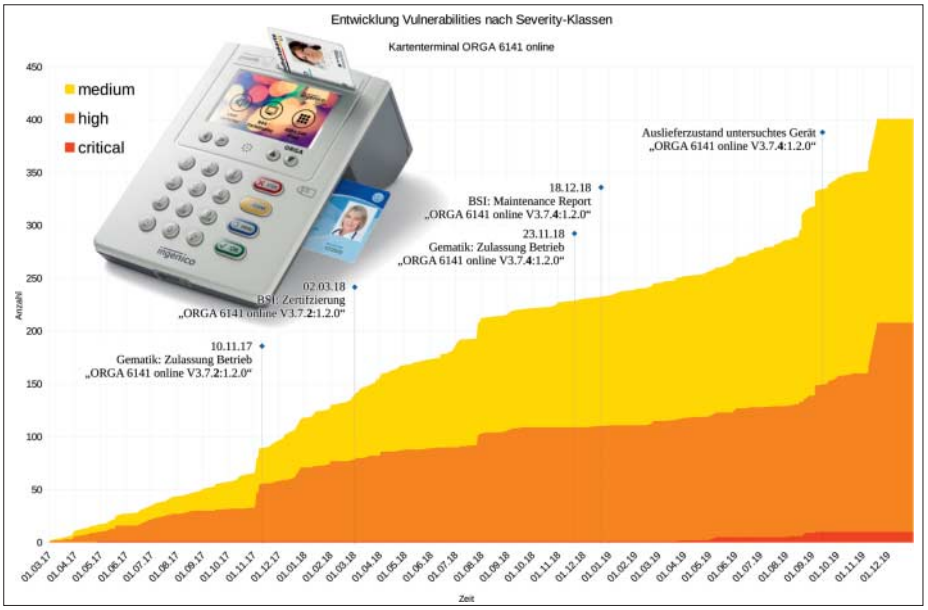

Bild: Thomas Maus

Die Grafik zeigt das Ansteigen der bekannt gewordenen Sicherheitslücken der Open-Source-Komponenten, die auch beim Kartenterminal Ingenico ORGA 6141 online (Firmware 3.7.4, Hardware-Revision 1.2.0) zum Einsatz kommen.