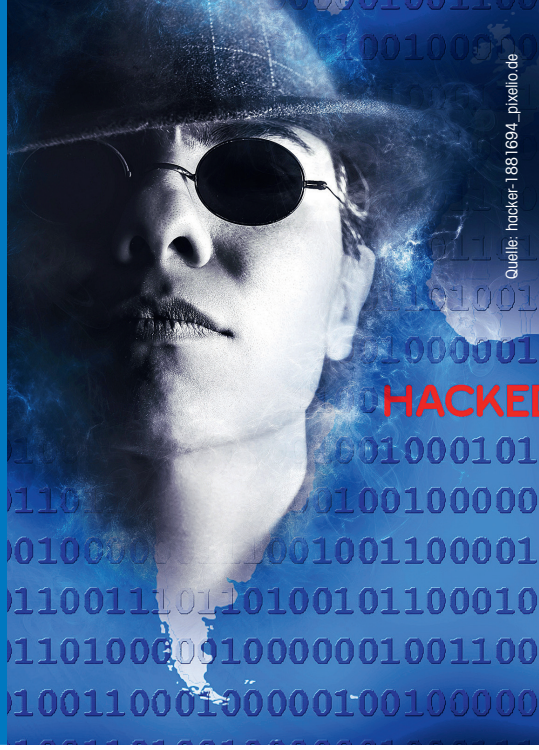
Cyberkriminalität mit vielen neuen Einfallstoren

Von Swantje Benkelberg



Quelle: hacker-1881694_pixelio.de

Der neue Bericht des Bundesamts für die Sicherheit in der Informationstechnik über die Lage der IT-Sicherheit in Deutschland hält auch für Banken und Versicherer trotz aller Bemühungen zur Verbesserung der Sicherheit einiges an Unerfreulichem bereit: Die mobile TAN lässt sich auf verschiedene Arten manipulieren. Und die Video-Identifikation ist nicht sicher, weil über diesen Kanal nicht alle Sicherheitsmerkmale des Ausweises überprüft werden können. Die größten Unwägbarkeiten birgt aber das Internet der Dinge. Denn hier ergibt sich eine ganze Reihe von Szenarien, die auch die Finanzbranche schädigen können. Und die vernetzten Geräte sind noch kaum gegen Angriffe gesichert.

Es ist eine Binsenweisheit: Mit der zunehmen der Digitalisierung mittlerweile fast aller Lebensbereiche wachsen auch die Angriffsstellen für Cyberkriminalität. Das geht einmal mehr aus dem Bericht „Die Lage der IT-Sicherheit in Deutschland 2017" hervor, den das Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, am 8. November vorgestellt hat.

Mit Blick auf Finanzdienstleister geht es inzwischen um weit mehr als das bloße „Phishing", mit dem Benutzer dazu gebracht werden sollen, ihre Zugangsdaten (etwa zu Internet-Banking, Bezahldiensten, sozialen Netzwerken oder Einkaufsportalen) auf Webseiten unter der Kontrolle der Angreifer einzugeben.

Das hat auch die Aufregung um Schwachstellen des Sicherheitsstandards WPA2 gezeigt, der Mitte Oktober die Gemüter erregte, als das BSI Verbraucher dazu riet, WLAN-Netzwerke bis zur Verfügbarkeit von Sicherheitsupdates nicht für Online-Transaktionen wie Online-Banking und Online-Shopping oder zur Übertragung anderer sensitiver Daten zu nutzen. Die Warnung mag übertrieben gewesen sein, wie eine Reihe von Sicherheitsexperten damals kommentierte. Dennoch zeigt die Tatsache, dass alle aktiven WLAN-fähigen Endgeräte in unterschiedlichen Ausprägungen von der Möglichkeit zum „Mitlesen" von Informationen betroffen sein können, das Ausmaß potenzieller Risiken.

Online-Banking-Betrug über Botnetze

Das gleiche Bild zeichnen auch die in dem BSI-Bericht genannten Zahlen zu Botnetz-Infrastrukturen, die 2016 und 2017 im großen Stil zum Informationsdiebstahl, für Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) auf Computersysteme, zum Spamversand und zur Verteilung von Schadprogrammen genutzt wurden.

- Täglich bis zu 27 000 Botinfektionen deutscher Systeme haben die Sicherheitsbehörden im Berichtszeitraum registriert und über das BSI an die deutschen Internet-Provider gemeldet, die dann wiederum ihre Kunden über die Infektion informieren und zum Teil auch Hilfestellung bei der Bereinigung der Systeme anbieten.

- Und eine genauere Betrachtung der zwanzig häufigsten Botnetz-Familien Anfang März 2017 zeigte, dass der Großteil davon vorrangig zum Online-Banking-Betrug verwendet wird.

Risiken bei der SMS-TAN

Jede sechste beobachtete Botnetz-Familie für Windows-Geräte verfügt ebenfalls über eine Schadsoftwarekomponente für Android-Systeme. Sie werden überwiegend beim Online-Banking-Betrug genutzt, um beim m-TAN-Verfahren die per SMS gesendete Transaktionsnummern abzufangen.

Die zunehmende Nutzung von SMS als Authentifizierungsfaktor sowie zur Autorisierung von Transaktionen (m-TAN-Verfahren) birgt deshalb durchaus Risiken, warnt da BSI. Angreifer können durch die Ausnutzung von Schwachstellen in der Netzwerkinfrastruktur den SMS-Verkehr umleiten und so die verschickten Codes missbrauchen. So gab es im Berichts-

zeitraum etwa Schwachstellen im für den Austausch zwischen Mobilfunknetzen wichtigen SS7-Protokoll und damit die Möglichkeit, SMS-Nachrichten beim Online-Banking abzufangen. Ein entsprechender Missbrauch ist auch durch Schadsoftware auf dem Endgerät möglich.

Video-Identifikation mit Missbrauchspotenzial

Neue Sicherheitsrisiken schon bei der Identifikation der Kunden gibt es durch den Vormarsch der Online-Identifikation. Mit der Online-Ausweisfunktion des Personalausweises könne zwar ein hohes Sicherheitsniveau erreicht werden, heißt es in dem Bericht. Die Verfahren der Video-Identifikation können laut BSI allerdings nicht das Niveau einer persönlichen Identifizierung und Überprüfung eines Ausweisdokuments erreichen – eine Botschaft, die Kreditinstitute und ihre auf eben diese Verfahren spezialisierten Dienstleister wohl nicht gerne hören werden.

Missbrauchspotenzial sieht die Behörde vor allem aufgrund der Tatsache, dass ein mit dem Smartphone aufgenommenes Videobild des Nutzers und seines Ausweises in Bezug auf Eindeutigkeit und Sicherheit nicht vergleichbar mit einer Identifizierung bei physischer Anwesenheit ist.

- Das liegt nicht zuletzt daran, dass sich über einen Videokanal höchstens Sicherheitsmerkmale prüfen, die sich bei bestimmten Lichtverhältnissen unter Bewegung des Ausweises verändern, wie das holografische Porträt oder das Laserkippbild auf der Rückseite des deutschen Personalausweises.

- Haptische Merkmale oder auch die nur im infraroten oder ultravioletten Licht erscheinenden Sicherheitsmerkmale hingegen können aus der Ferne nicht überprüft werden.

Inwieweit dadurch Missbrauch möglich ist, hat das BSI im Rahmen von Sicherheitsanalysen untersucht. Tatsächlich wurde dabei nachgewiesen, dass es bereits mit einem Standardequipment effektiv möglich ist, einen gefälschten Ausweis zu erstellen und im Rahmen einer Videoübertragung in Echtzeit den Eindruck entsprechender individueller, optisch variabler Sicherheitsmerkmale zu erzeugen.

Ob so etwas künftig zu einem Verbot der Videoidentifikation führen wird, was in der Nutzerfreundlichkeit einer Rolle rückwärts gleichkäme, oder ob und wie die Verfahren angepasst werden können und müssen, um ein Mehr an Sicherheit zu erreichen, wird sich vermutlich erst noch zeigen – auch abhängig davon, wie häufig es an dieser Stelle tatsächlich zu Betrugsfällen kommt.

Internet der Dinge mit vielfältigen Gefahren

Das Haupteinfallstor für Cyberkriminelle – noch dazu eines, das bislang weitgehend offen steht –, scheint dem Bericht zufolge künftig aber das Internet der Dinge zu sein. Denn die IT-Sicherheit spielt bei vernetzten Geräten bisher keine oder nur eine untergeordnete Rolle. Sondern für eine Kaufentscheidung des Kunden sind in der Regel die Gerätefunktionalität und der damit verbundene Komfortgewinn sowie der Kaufpreis ausschlaggebend. Dies führt dazu, dass mit den an internetfähigen Haushaltsgeräten oder Fahrzeugen ein ganz neuer Bereich der Gefährdung entsteht, die von Cyberkriminellen genutzt werden kann.

Die Angriffe auf IoT-Geräte erfolgen in der Regel direkt über das Internet oder über vorhandene Funkschnittstellen „over-the-air". Hierbei macht das BSI verschiedene Gefährdungslagen mit unterschiedlichen Bedrohungen aus:

- Das IoT-Gerät wird angegriffen, um dem Nutzer direkten Schaden zuzufügen. So können zum Beispiel Smart-Home-Komponenten zur Zutrittssteuerung angegriffen und manipuliert werden, um einen Einbruch vorzubereiten. Oder über eine kompromittierte Webcam können vertrauliche Informationen über die Bewohner und deren Verhalten in Erfahrung gebracht werden.
- Das IoT-Gerät wird kompromittiert und zum Angriff auf andere Infrastrukturkomponenten oder Services missbraucht. Häufig werden ungesicherte oder nicht ausreichend gesicherte IoT-Geräte kompromittiert und zu Botnetzen zusammengeführt, um gezielte DDoS-Attacken gegen Webseiten oder Webservices von Dritten durchzuführen. Hierbei bleibt der Angriff für den Nutzer häufig unentdeckt, da er selbst von dessen Auswirkungen nicht direkt betroffen ist.
- Das IoT-Gerät wird durch ein Schadprogramm außer Betrieb gesetzt und ist für den Endnutzer zumindest vorübergehend nicht mehr nutzbar. Hiervon waren in jüngster Vergangenheit speziell kleine und mittelständische Unternehmen (KMUs) betroffen, deren Infrastruktur teils tagelang über das Internet nicht mehr erreichbar war.

Mannigfache Implikationen für die Finanzbranche

Die möglichen Auswirkungen solcher Cyberangriffe sind vielfältig. Die Finanzbranche ist davon nur auf den ersten Blick nicht betroffen. Bei genauerer Hinsicht ergibt sich jedoch auch für Finanzdienstleister eine ganze Reihe von Implikationen.

Zum einen sind das die neuen „Bezahlsituationen", auf die sich die Kartenorganisationen mit den APIs für Drittanbieter einstellen. Wenn über das Fahrzeug, die Waschmaschine oder den Kühlschrank Bestellungen ausgelöst werden können, dann bieten sich hier auch neue Sicherheitslücken, die sich nicht einfach werden schließen lassen. Schließlich bieten Tools wie der „Dash-Button" von Amazon, mit dem der Kunde per Knopfdruck an der Waschmaschine Waschmittel nachordern kann, dem Kunden nur dann einen Mehrwert, wenn sie nicht mit einem aufwendigen, mehrstufigen Sicherheitsverfahren verknüpft sind.

Wenn Heizung, Rollläden, Spülmaschine und Fernseher mit dem Internet verbunden werden, vervielfacht sich darüber hinaus die Anzahl der möglichen Geräte, die – einmal kompromittiert – zu Botnetzen zusammengeschlossen werden können. Angesichts der Tatsache, dass solche Botnetze zum großen Teil für den Online-Banking-Betrug verwendet werden, dürfte sich daraus eine exponentielle Steigerung des Angriffspotenzials ergeben.

Angriffe, durch die kleine oder mittelgroße Unternehmen im schlimmsten Fall für eine Weile lahmgelegt werden, die Existenz gefährden oder zumindest die Fähigkeit einschränken, Kredite zu bedienen. Dass Cyber-Schutz-Policen hier ein wachsende Thema sind, ist die logische Folge.

Vergleichsweise offensichtlich sind deshalb die Gefahren für die Versicherungswirtschaft: Wenn etwa gehackte Haushaltsgeräte oder eine Webcam Auskunft über Gewohnheiten der Bewohner einer Wohnung geben und die Kriminellen dann zusätzlich Zugriff auf das Zugangssystem erhalten, dann steigt nicht nur das Einbruchsrisiko – sondern damit auch die Schadenbelastung der Versicherer. Und dafür muss es nicht unbedingt die professionelle Einbrecherbande sein.

Damit sich Schäden durch Cyberkriminalität bei den Versicherern häufen, kann es schon genügen, wenn „Spaßvögel" technische Geräte so manipulieren, dass diese dadurch Schaden nehmen. Die Kalkulation von Policen zur Absicherung solcher und anderer möglicher Schäden durch Cyberkriminalität wird deshalb wohl eine Aufgabe, die die Aktuare in nächster Zeit intensiv beschäftigen wird.