PANDALABS REPORT
Q3 2016

panda

pandalabs

1. EINFÜHRUNG

1 EINFÜHRUNG

Die Cyberkriminalität wird so bald nicht zurückgehen. Im dritten Quartal 2016 waren die Cyberkriminellen noch weitaus erfindungsreicher als zuvor und nutzten innovative Technologien und neue Tools, um ihre Malware zu verbreiten. PandaLabs, Panda Securitys Anti-Malware-Labor, hat allein in diesem Quartal mehr als 18 Millionen neue Malware-Exemplare entdeckt. Das sind durchschnittlich 200.000 Samples pro Tag und ein Beweis dafür, dass die alarmierenden Probleme mit der Internetkriminalität weiterhin bestehen.

Trojaner stehen in diesem Quartal als beliebteste Malware an der Spitze, wobei Ransomware den Hauptteil ausmacht.

Ransomware-Angriffe haben im dritten Quartal 2016 enorm zugenommen und Cyberkriminelle streichen Millionen von Dollar ein.

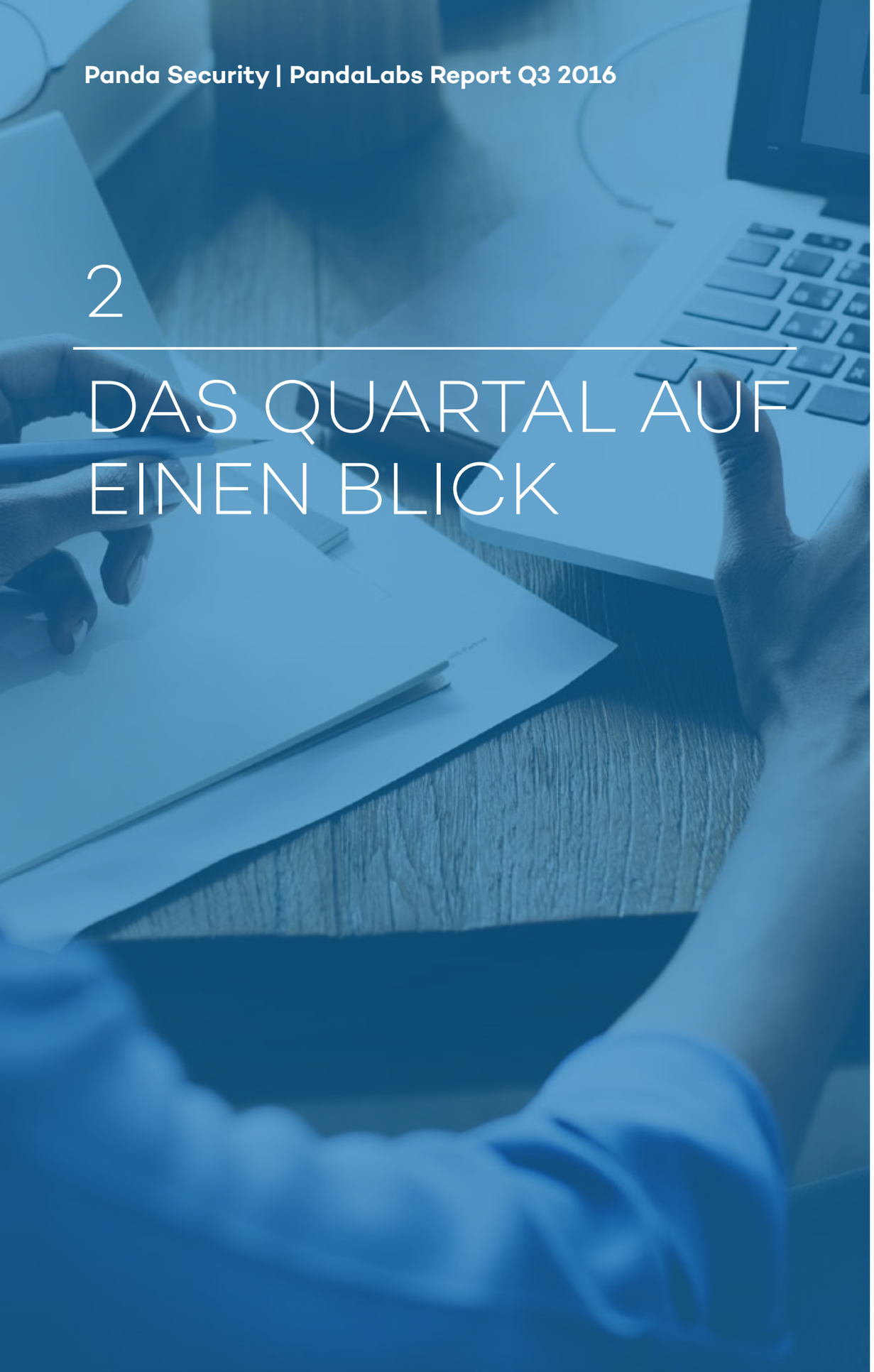
POS-Terminals in Hotels, Restaurants und anderen Einrichtungen werden für Cyberkriminelle immer interessanter.

Die Informationen, die wir in den vergangenen drei Monaten durch das Klassifizieren und Analysieren von Malware gesammelt haben, zeigen, **dass eine Reihe von massiven DDoS-Attacken** (Distributed Denial of Service) stattgefunden haben. In vielen Fällen werden sie von einem Botnetz ausgeführt, das nicht aus Computern sondern aus smarten Geräten, wie zum Beispiel IP-Kameras, besteht.

In unserem Report werden wir ausführlich auf die jüngsten Angriffe eingehen, die gegen das Internet der Dinge (IoT) gerichtet waren, wie zum Beispiel die Hackerangriffe, von denen **vernetzte Autos** angesehener Hersteller wie Jeep und Tesla betroffen waren. Im Rahmen einer Untersuchung wurde demonstriert, wie ein Tesla-Modell ohne physischen Kontakt ferngesteuert werden kann.

Im Bereich der Mobiltelefone werden wir verschiedene Situationen analysieren, zu denen Angriffe auf Android-Geräte gehören. Außerdem zeigen wir, wie sich eine Welle von Ransomware-Angriffen gegen iOS-basierte Geräte richtet.

2. DAS QUARTAL AUF EINEN BLICK



2

DAS QUARTAL AUF EINEN BLICK

Ransomware

Ransomeware ist ein Geschäft, das Kriminellen hohe Profite verspricht. Je technisch ausgereifter und komplexer diese Malware wird, desto höher werden auch die Einnahmen sein. Im Juli begannen die Erfinder der Petya und Mischa Ransomware damit, Malware und entsprechende Bezahlplattformen zu entwickeln, während sie deren Verbreitung Dritten überließen. Dieses neue Modell nennt sich **Ransomware as a Service (RaaS).**

Bei RaaS kreieren Entwickler die Ransomware, während Distributoren für das Infizieren der Opfer verantwortlich sind. Wie bei der Verteilung legaler Programme können sie höhere Gewinnspannen durch ein hohes Geschäftsvolumen erzielen. Je mehr Opfer infiziert und je mehr Lösegelder gezahlt werden, desto höher ist der Gehaltsscheck für die Distributoren. Ihre Gewinne beginnen gewöhnlich bei 25 Prozent, doch kann ein Distributor ihn unter Umständen auf bis zu 85 Prozent erhöhen, wenn es ihm gelingt, **mehr als 125 Bitcoins** (ca. 75.000 US-Dollar) pro Woche zu **erpressen.**

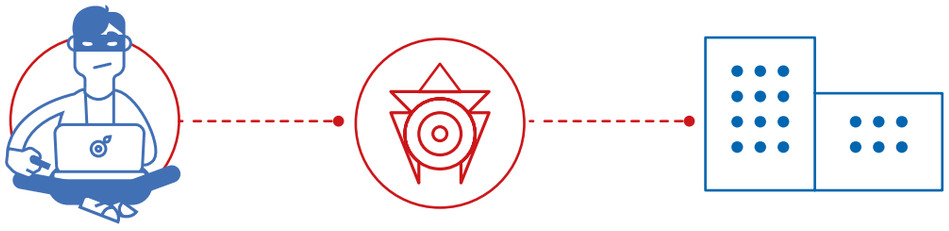
Die Mitarbeiter des PandaLabs verfolgen die Entwicklung von Ransomware sehr genau. Alle zwei Monate veröffentlichen wir Artikel im Panda Security Media Center unter der Rubrik „Tales from Ransomwhere“, in denen die Leser alles über die neuesten Entwicklungen in Bezug auf diese Angriffe erfahren. Wir haben analysiert, wie Angreifer PowerShell benutzen und missbrauchen, um Ransomware-Attacken zu starten – und zwar ohne Dateien aus dem Internet oder aus Word-Dokumenten mit Makros, die per E-Mail versandt wurden, herunterladen zu müssen. (PowerShell ist ein Programm, das standardmäßig von Windows 10 mitgeliefert wird.)

Großangelegte Ransomware-Angriffe haben wir zum Beispiel mit den sogenannten Locky-Trojanern erlebt.

Diese Schadsoftware implementiert einen „Offline“-Modus, der es ihr ermöglicht, Dateien zu verschlüsseln, auch wenn Schutzlösungen sie vielleicht daran hindern mit dem Server zu kommunizieren, der das Verschlüsselungspasswort liefert.

Neben den traditionellen Infektionstechniken mittels Exploits und Spam gibt es andere äußerst effektive Techniken, die sich speziell gegen Unternehmen richten.

Im September erlebten wir, wie eine Gruppe von Angreifern erfolgreich die Ransomware Crysis auf dem Server einer französischen Firma installierte.



Bei der Untersuchung des Vorfalls stellte sich heraus, dass der Server den Remote Desktop Protocol Service mit dem Internet verbunden hatte. Die Angreifer versuchten vier Monate lang mithilfe einer Brute-Force-Attacke in den Server einzudringen. Nach mehr als 100.000 Versuchen gelang es ihnen schließlich, die Anmeldedaten zu finden.

Cyberkriminalität

Cyberkriminalität zu messen, ist sehr kompliziert. Cybersicherheitsexperten, die täglich gegen diese Bedrohungen kämpfen, wissen, dass dies eine Branche ist, die ständig wächst und sich weiterentwickelt.

Aber ist sie wirklich so gefährlich?

Einige Leute denken vielleicht, dass große IT-Sicherheitsunternehmen wie Panda Security besonders am Wachstum der Cyberkriminalität interessiert sind, weil ihr Geschäft von diesen Problemen profitiert. Die Daten sprechen jedoch für sich. Immer mehr unabhängige Organe liefern Statistiken, die uns dabei helfen, die aktuelle Lage der Cyberkriminalität einzuschätzen.

Die National Crime Agency (NCA) Großbritanniens hat einen Bericht veröffentlicht, der zeigt, dass die Internetkriminalität derzeit mehr als 50 Prozent der verübten Verbrechen in Großbritannien ausmacht.

Einer der größten Bitcoin-Raubzüge der Geschichte ereignete sich am 2. August 2016. Bitcoins im Wert von 60 Millionen Dollar wurden der Bitcoin-Börse Bitfinex gestohlen. Das Geld gehörte Kunden, die Bitcoins bei dieser „Bank“ deponiert hatten. Es gibt immer noch keine Hinweise darauf, wer diesen Angriff ausgeführt hat. Bitfinex hat auch keinerlei Informationen darüber preisgegeben, wie sich diese Attacke ereignet haben könnte. Strafverfolgungsbehörden führen derzeit eine Untersuchung durch.

Im September enttarnte der amerikanische Journalist und Sicherheitsforscher Brian Krebs vDOS, ein „Unternehmen“, das DDoS-Attacken als Dienstleistung anbietet.

Kurz nach der Enthüllung wurden die vDOS-Angreifer verhaftet. (Sie waren in der Lage, innerhalb von zwei Jahren 150.000 Angriffe zu starten und einen Gewinn von 618.000 Dollar zu erzielen.) Nach ihrer Verhaftung dauerte es nicht lange, bis die Webseite von Brian Krebs Opfer einer massiven DDoS-Attacke wurde, woraufhin er diese für eine Woche vom Netz nahm. Schließlich schaltete sich Google ein und schützte seine Webseite durch Project Shield, sodass sie wieder funktionierte. Krebs geht in seinem Artikel, der unter dem Titel „Die Demokratisierung der Zensur“ veröffentlicht wurde, näher auf die möglichen Auswirkungen dieser Attacken ein.

Die Battle.net-Server von Blizzard wurden von einer Gruppe mit dem Namen PoodleCorp angegriffen, die drei Spiele kompromittierte (World of Warcraft, Overwatch, Diablo 3). Im Laufe des dritten Quartals gab es eine Reihe ähnlicher Angriffe. Wir werden im Abschnitt „Internet der Dinge“ näher darauf eingehen, da ein Großteil dieser Attacken mithilfe von Botnetzen gestartet wurde, die aus smarten Geräten wie IP-Kameras, Routern usw. bestehen.

Von Juli bis September 2016 gab es viele Datendiebstähle, von denen Millionen Anwender weltweit betroffen waren. Im Juli wurden die Ubuntu-Foren gehackt, in denen User alle Aspekte des auf GNU/Linux basierenden Open-Source-Betriebssystems diskutieren. Es wurden die E-Mail-Adressen, Benutzernamen und IP-Adressen von zwei Millionen Personen gestohlen. Black Hats griffen auch Foren an, die mit dem beliebten Handyspiel **Clash of Kings** verbunden sind. In diesem Fall **stahlen die Angreifer die persönlichen Daten von 1,6 Millionen Spielern.** Nutzer des von Valve entwickelten Spiels Dota 2 wurden in diesem Quartal ebenfalls Opfer eines Angriffs. Ihr Forum wurde gehackt und es wurden persönliche Informationen wie Anmeldedaten und E-Mail-Adressen von 1,9 Millionen Usern gestohlen. Dieselben Angreifer stahlen 9 Millionen Steam Game Codes, nachdem sie die DLH.net-Webseite gehackt hatten.

Cyberkriminelle stießen auf eine Goldgrube als sie damit begannen, Spieleseiten zu hacken.

Zu dieser Liste können wir Folgendes hinzufügen: Die Daten von 200.000 GTA-Gaming.com-Nutzern wurden gestohlen, www.minecraftworldmap.com wurde angegriffen und die Angreifer veröffentlichten die Daten von 71.000 Anwendern.

Eine weitere brisante Attacke richtete sich gegen die **pornografische Webseite Brazzers.** Bei dieser Sicherheitsverletzung wurden die **Daten von 800.000 Nutzern** gestohlen. Ein weiterer herausragender Angriff betraf den Instant-Messaging-Service QIP.ru, bei dem die Daten von 33 Millionen Anwendern gestohlen wurden.

Auch Dropbox entkam den Fängen der Cyberkriminellen nicht. Der bekannte File-Sharing-Dienst stellte erst kürzlich fest, dass er 2012 Opfer einer Cyberattacke geworden war.

Die Folge: Die Nutzerdaten von 68 Millionen Anwendern gingen verloren. Ein Raub, den wir wohl nicht vergessen werden, betraf **Yahoo.** Obwohl er sich bereits 2014 ereignete, war davon bis jetzt nichts bekannt. Insgesamt **500 Millionen Konten wurden gehackt, was ihn zum bisher größten Diebstahl seiner Art macht.**

POS-Terminals sind ein weiterer Bereich, auf den sich Cyberkriminelle heutzutage konzentrieren.

PandaLabs entdeckte eine Attacke, bei der **200 amerikanische Einrichtungen** kompromittiert wurden, die meisten davon Restaurants. Mithilfe der **Malware PunkeyPOS** wurden Kredit- und Debitkarteninformationen gestohlen.

Die beliebte Fast-Food-Kette Wendy's wurde Opfer eines ähnlichen Angriffs, bei dem POS-Terminals in mehr als 1.000 Filialen durch eine Variante von PunkeyPOS infiziert wurden.

Unser Labor entdeckte eine weitere ähnliche Attacke. Wieder einmal waren amerikanische Restaurants die Opfer.

In diesem Fall wurden **300 POS-Terminals** mit der **Malware PosCardStealer** infiziert.

Ein weiterer kritischer Bereich, den wir in einem vorherigen PandaLabs-Bericht untersucht haben, ist die Hotelbranche.

In diesem Quartal wurde eine Reihe von HEI-Hotels angegriffen. Die Kriminellen setzten Malware ein, um Kreditkarten-informationen von den POS-Terminals der Hotels zu stehlen. Davon betroffenen waren Sheraton, Westin, Hyatt und Marriot.

Doch die Cyberkriminellen haben ein Ziel ins Auge gefasst, das anspruchsvoller ist als POS-Terminals. Im Juli wurden Dutzende Geldautomaten der First Bank in Taiwan ausgeraubt. Dieses Verbrechen lief organisiert ab. Die Angreifer warteten neben jedem Geldautomaten, während sie insgesamt 2 Millionen Dollar abhoben. Wir wissen, dass die Verbrecher Malware auf diesen GAAs installiert hatten (sicherlich nach dem Hacken des internen Netzwerkes der Bank) und dann das Geld entnahmen, ohne die Geldautomaten zu berühren, indem sie Remote-Befehle nutzten, wie das Bildmaterial der Sicherheitskameras zeigt.

Belohnungsprogramme für diejenigen, die Schwachstellen finden.

Der Technologiegigant **Apple** ist eines der Unternehmen, die erst vor kurzem ein Belohnungsprogramm ins Leben gerufen haben. Sie bieten IT-Experten bis zu 200.000 Dollar, wenn es ihnen gelingt, Schwachstellen in Apple-Produkten zu finden.

Interessanterweise haben viele verschiedene Unternehmen derartige Belohnungsprogramme. Obwohl sie normalerweise Geldprämien vergeben, gibt es einige Firmen, die eine andere Form der Bezahlung bieten, wie zum Beispiel **United Airlines.** Im August wurde bekannt, dass das Unternehmen einen Sicherheitsspezialisten mit **einer Million Bonusmeilen** aus seinem Treueprogramm belohnte, weil er 20 Sicherheitslücken in der Software entdeckt hatte. White-Hat-Hacker von Offensi.com erhielten ebenfalls Flugmeilen, die sie großzügig für drei Wohltätigkeitsorganisationen spendeten.

Hohe Strafen für Cyberkriminelle

Im Juli wurden in London fünf Mitglieder einer Geldwäscherbande verhaftet. Zu den fünf Russen gehörten auch die Anführer der Gang, der 30-jährige Aslan Abazov und der 29-jährige Aslan Gergov. Abazov wurde zu 7,5 Jahren und Gergov zu 7 Jahren und 3 Monaten Gefängnis verurteilt.

Edward Majerczyk bekannte sich des Diebstahls von Promifotos schuldig und handelte damit einen Deal aus, der ihm nur 9 Monate Gefängnis einbrachte statt der vom Staatsanwalt ursprünglich geforderten 5 Jahre. Majerczyk gab zu, dass er Zugriff auf die iCloud-Konten der Opfer erlangte, nachdem er eine Phishing-Attacke gestartet hatte, um ihre Anmeldedaten zu bekommen.

Einige Leute sehen es als große Leistung an, die Accounts von Personen des öffentlichen Lebens zu hacken. So war es auch im Fall von Marcel Lehel Lazar, einem 44-jährigen Rumänen. Er wurde zu einer Gefängnisstrafe von 52 Monaten verurteilt, weil er zahlreiche einflussreiche Personen gehackt hatte. Zu seinen 100 Opfern gehörten Hillary Clinton, George Bush (Vater und Sohn), Colin Powell, Nicole Kidman und Robert Redford.

Mobile Malware

Android-Geräte stehen in der Schusslinie. Die Menschen kaufen sich weiterhin Smartphones und Cyberkriminelle nehmen sie nach wie vor ins Visier. Da das Android-Betriebssystem den größten Marktanteil hat und es Anwendern erlaubt, Programme zu installieren, die nicht aus dem offiziellen App-Store sind, ist es für Kriminelle ein leichteres Ziel. Doch glücklicherweise ist Google dabei, die Sicherheit zu verstärken. Verschiedene Sicherheitsmaßnahmen (die aus den neuesten Versionen von Linux Kernel stammen) werden in der 7. Version des Android-Betriebssystems „Nougat“ aktiviert.

Wie sicher sie auch sein mögen, in vielen Fällen sind diese Schutzmaßnahmen nicht ausreichend. Das Sicherheitsunternehmen Checkpoint entdeckte **vier Sicherheitsprobleme, die 900 Modelle der Android-Geräte gefährden könnten, die mit Qualcomm Snapdragon Prozessoren ausgerüstet sind.**

Gugi, ein Android-Trojaner, kann die Sicherheitsbarrieren von Android 6 überspringen; das heißt, er kann Bankdaten und Informationen von anderen Anwendungen stehlen, die auf diesen Geräten installiert sind.

Wie gelingt dem Trojaner das? Wenn Anwender eine legale App benutzen, legt Gugi einen anderen Bildschirm darüber und verlangt Informationen, die ohne das Wissen der Opfer direkt an die Cyberkriminellen gesendet werden.

Neuerdings nehmen die Ransomware-Angriffe auf iPhones und iPads zu. Aber die Cyberkriminellen benutzten für diese Angriffe keine Malware wie bei Windows-Geräten. Um den Angriff ausführen zu können, verwendeten sie stattdessen die Apple-ID des Opfers sowie sein Passwort (an die sie wahrscheinlich durch Phishing gelangten oder durch die Wiederverwendung von Passwörtern unterschiedlicher Webseiten). Sie aktivierten den Lost-Modus in der Anwendung „Find my iPhone“ und fügten eine Mitteilung hinzu, in der sie ein Lösegeld in Bitcoins verlangten, statt das Passwort herauszugeben, das für das Entsperren des Telefons benötigt wird.

Im August brachte Apple die iOS-Version 9.3.5 für Mobilgeräte heraus. Diese Version behebt drei Zero-Day-Schwachstellen, die von einer Spyware mit dem Namen Pegasus ausgenutzt werden. Pegasus wurde von der NSO-Gruppe entwickelt, einem israelischen Unternehmen, das ähnliche Produkte anbietet wie das Hacking Team.

Internet der Dinge

Auf der Hacker-Konferenz DEF CON, die jedes Jahr in Las Vegas stattfindet, demonstrierte der Sicherheitsforscher Andrew Tierney, wie er die Kontrolle über ein Thermostat übernehmen konnte, das er selbst modifiziert hatte. Nachdem er eine SD-Karte in das Thermostat eingesetzt hatte, stieg die Temperatur auf ca. 37 °C. Es konnte nur mit einer PIN wieder deaktiviert werden. Es handelte sich um ein vernetztes Thermostat, auf dessen Display die Forderung erschien, einen Bitcoin zu zahlen, um die Kontrolle zurückzuerhalten. Obwohl dies nur ein Machbarkeitsnachweis war, der direkten Zugriff auf das Gerät erforderte, erhalten wir doch eine Vorstellung davon, mit welchen Angriffen auf vernetzte Haushaltsgeräte wir in den kommenden Jahren konfrontiert werden könnten.

Tatsächlich gibt es bereits Millionen Geräte im Internet der Dinge, die schon gehackt wurden. Mithilfe eines Botnetzes aus kompromittierten Heim-Routern führte die Hackergruppe Lizard Squad während der Feiertage eine verheerende DDoS-Attacke auf die Playstation- und Xbox-Dienste aus. Laut Aussage des Sicherheitsexperten Brian Krebs sei dies eine Werbeaktion für das DDoS-Tool „Lizard Stresser“ des Hacker-Teams gewesen.

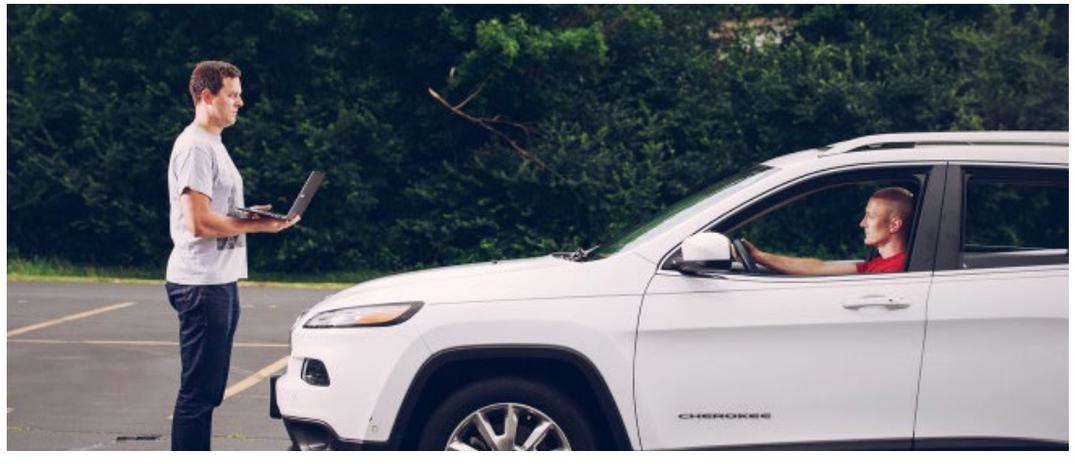
Nach Auskunft von Arbor Networks bilden IP-Kameras die Mehrheit dieser vernetzten Geräte. Sie können ganz einfach gehackt werden, indem man verschiedene Benutzername-Passwort-Kombinationen ausprobiert. Da die meisten Anwender die Standardanmeldedaten des Herstellers nicht ändern, ist es leicht, Zugriff auf die Geräte zu erhalten. Tatsächlich wurden bereits Attacken mit bis zu 400 Gbps gestartet. Andere beliebte Geräte, die schon seit langer Zeit für diese Art der Angriffe genutzt werden, sind Router.

Ende September erlitt der französische Hosting Provider OVH eine 1Tbps-DDos-Attacke – die wahrscheinlich größte Offensive, die es bisher gegeben hat. Octave Klaba erklärte, dass die Server des Unternehmens gleichzeitig von mehreren Angriffen, die 100 Gbps überschritten und zusammen 1 Tbps ausmachten, betroffen waren. Die schwerste Einzelattacke, die von OVH dokumentiert wurde, erreichte 93 MMps und 799 Gbps. Der Angriff wurde mithilfe von 152.000 Geräten ausgeführt, von denen die meisten zum Internet der Dinge gehörten (IP-Kameras, Videorekorder usw.).

Auch die Automobilindustrie ist betroffen. Sicherheitsforscher der **University of Birmingham demonstrierten**, wie sie die **funkgesteuerten Türschließsysteme aller Fahrzeuge, die von der Volkswagen-Gruppe** in den vergangenen 20 Jahren **verkauft wurden**, hacken konnten. Sie entdeckten eine Schwachstelle in den Funkschlüsseln. Den Sicherheitsforschern zufolge gibt es nur wenige Masterkeys, deren Verschlüsselung sie analysierten, wobei sie eine Systematik im Öffnungscode entdeckten. Autobesitzer können beim Abschließen ihres Fahrzeugs quasi „abgehört“ werden. Die Diebe können den Code abfangen und damit anschließend in das Auto eindringen.

Die Sicherheitsforscher **Charlie Miller** und **Chris Valasek**, die im vergangenen Jahr **zeigten, wie sie einen Jeep Cherokee remote hackten,** sind in diesem Jahr noch einen Schritt weitergegangen. Sie demonstrierten, wie sie Signale außer Kraft setzen und der Parkbremse befehlen konnten, sich nicht zu aktivieren. Außerdem deaktivierten sie das Lenkrad und brachten es dazu, sich auf Befehl mit jeder beliebigen Geschwindigkeit zu drehen. Um diese Art der Kontrolle zu erhalten, mussten sie allerdings einen Computer direkt an das Auto anschließen. Es ist sehr wichtig, dass wir besonderes Augenmerk auf diese lebensbedrohenden Hacks legen. Ihr Leben könnte in Gefahr sein, wenn es möglich ist, das Auto zu manipulieren, das Sie fahren.

Im September zeigten chinesische Sicherheitsforscher der Keen Security Labs, wie man ein Tesla-Fahrzeug aus der Ferne hacken kann, sowohl im Park- als auch im Fahrmodus. In ihrem Video kann man sehen, wie das Auto ferngesteuert werden kann, ohne es physisch zu berühren. Das Fahrzeug kann geöffnet und geschlossen werden, der Kofferraum kann während der Fahrt geöffnet werden und selbst die Fernsteuerung der Bremsen ist möglich. Die Sicherheitsforscher sendeten die Informationen vorher an den Hersteller, sodass er die entdeckten Probleme mit der neuesten Version der Firmware beheben konnte.



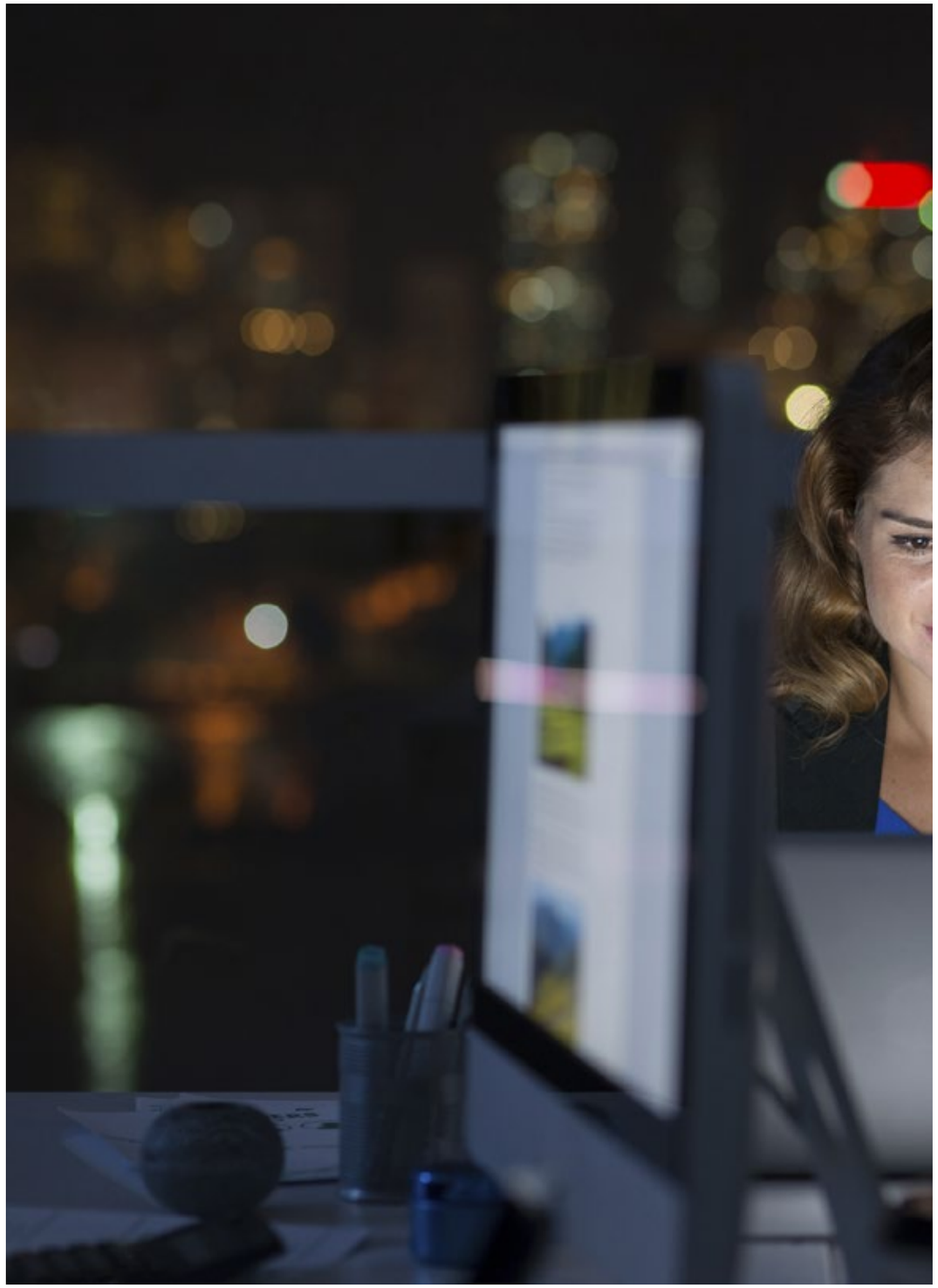
Cyberkrieg

Mitten in der Wahlkampagne zu den US-Präsidentschafts-wahlen gab es einen Angriff auf das **Democratic National Committee (DNC).** Bei dieser Cyberattacke wurden **alle Arten von hochsensiblen Daten gestohlen und veröffentlicht.** Während es normalerweise sehr schwierig und manchmal sogar unmöglich ist, herauszufinden, wer hinter diesen Attacken steckt, scheint es in diesem Fall klar zu sein, dass es sich um russische Angreifer handelte. Das führte zu den Beschuldigungen, die russische Regierung versuche, der DNC-Kampagne zu schaden. Offensichtlich gab es zwei unterschiedliche Angreifer (beide Russen) und einer von ihnen **veröffentlichte 20.000 E-Mails auf WikiLeaks.**

Bleiben wir beim Wahlthema: **Das FBI gab eine Warnmeldung heraus, die besagte, dass zwei Wahlwebseiten gehackt worden seien** und dass mindestens einer der ausländischen Angreifer in den Besitz von Informationen über die Wählerregistrierung gelangt sein könnte.

Regierungen erkennen, wie wichtig Cybersicherheit ist. US-Präsident Obama stellte fest, dass es noch viel zu tun gibt, insbesondere wenn man daran denkt, dass das Netzwerk des Weißen Hauses in der Vergangenheit gehackt worden ist. Im September ernannte er **den ersten CISO (Chief Information Security Officer) in der amerikanischen Geschichte.**

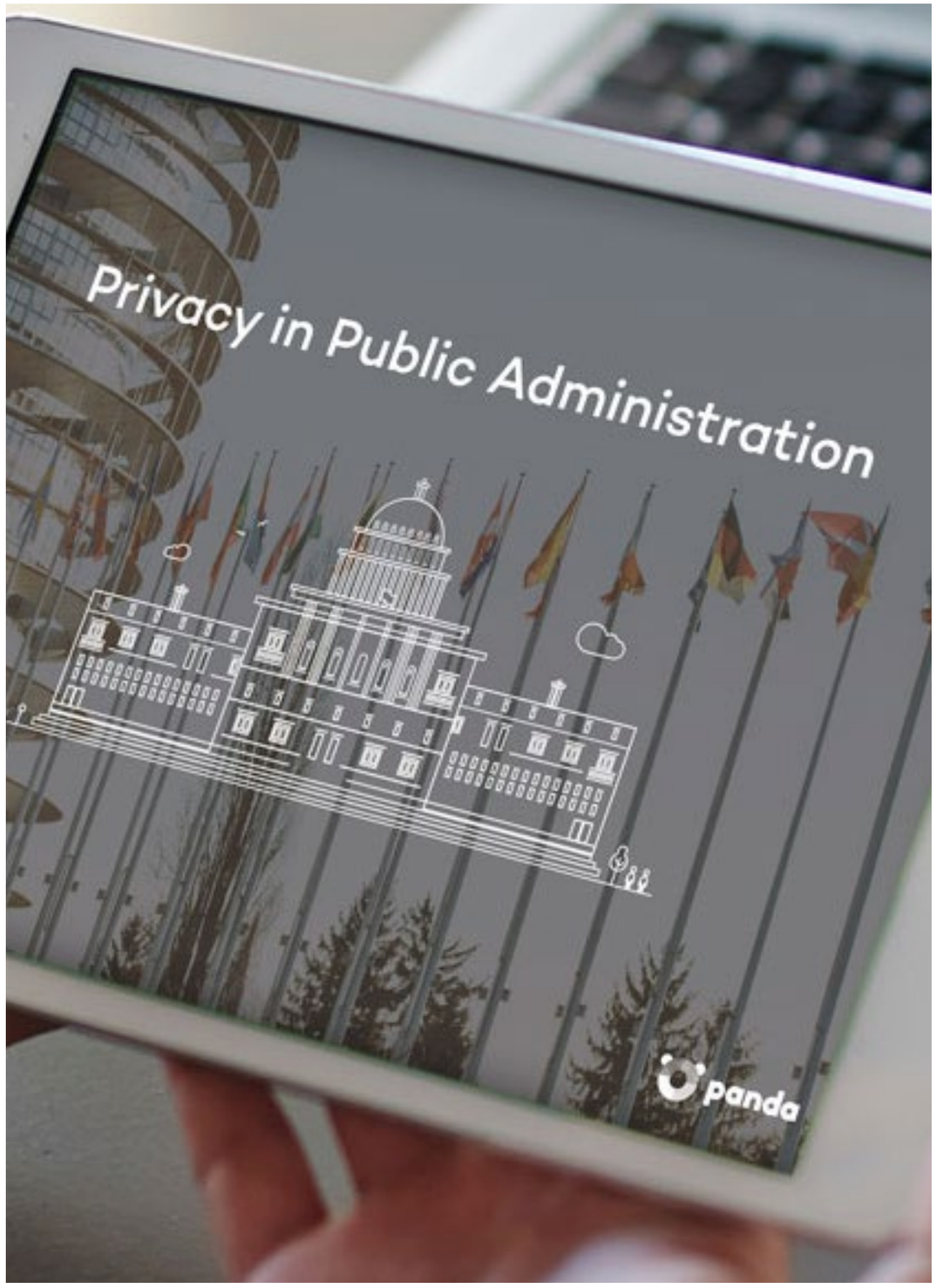
Im August **gab** eine Gruppe, die sich selbst „The Shadow Brokers“ nennt, bekannt, dass sie die **National Security Agency (NSA)** gehackt hätten. Sie machten einige der gestohlenen Cyberwaffen publik und versprachen, sie an den Meistbietenden zu verkaufen. Es ist immer noch nicht klar, wer hinter dem Angriff steckt.



Bei vielen Gelegenheiten haben wir über Angriffe gesprochen, die von Regierungen unterstützt wurden. Doch die Wahrheit ist, dass es bei Cyberverbrechen praktisch unmöglich ist, die Kriminellen zu identifizieren. Wir waren überrascht, zu hören, dass **Google** seine Kunden benachrichtigt, wenn Angriffe dieser Art entdeckt werden. Laut Aussage der leitenden Angestellten Diane Greene versendet Google **monatlich 4.000 solcher Benachrichtigungen.**

Südkoreanische Ankläger glauben, dass Nordkoreaner für **das Hacken Dutzender E-Mail-Accounts von Regierungsbeamten** verantwortlich seien.

Schlagzeilen machte die Information, dass der **Iran Malware in zwei petrochemischen Werken entdeckt und bereinigt** hat. **Es ist allgemein bekannt, dass es zuvor mehrere Feuer in diesen Werken gegeben hat.** Deshalb wird jetzt untersucht, ob diese durch Malware verursacht wurden.



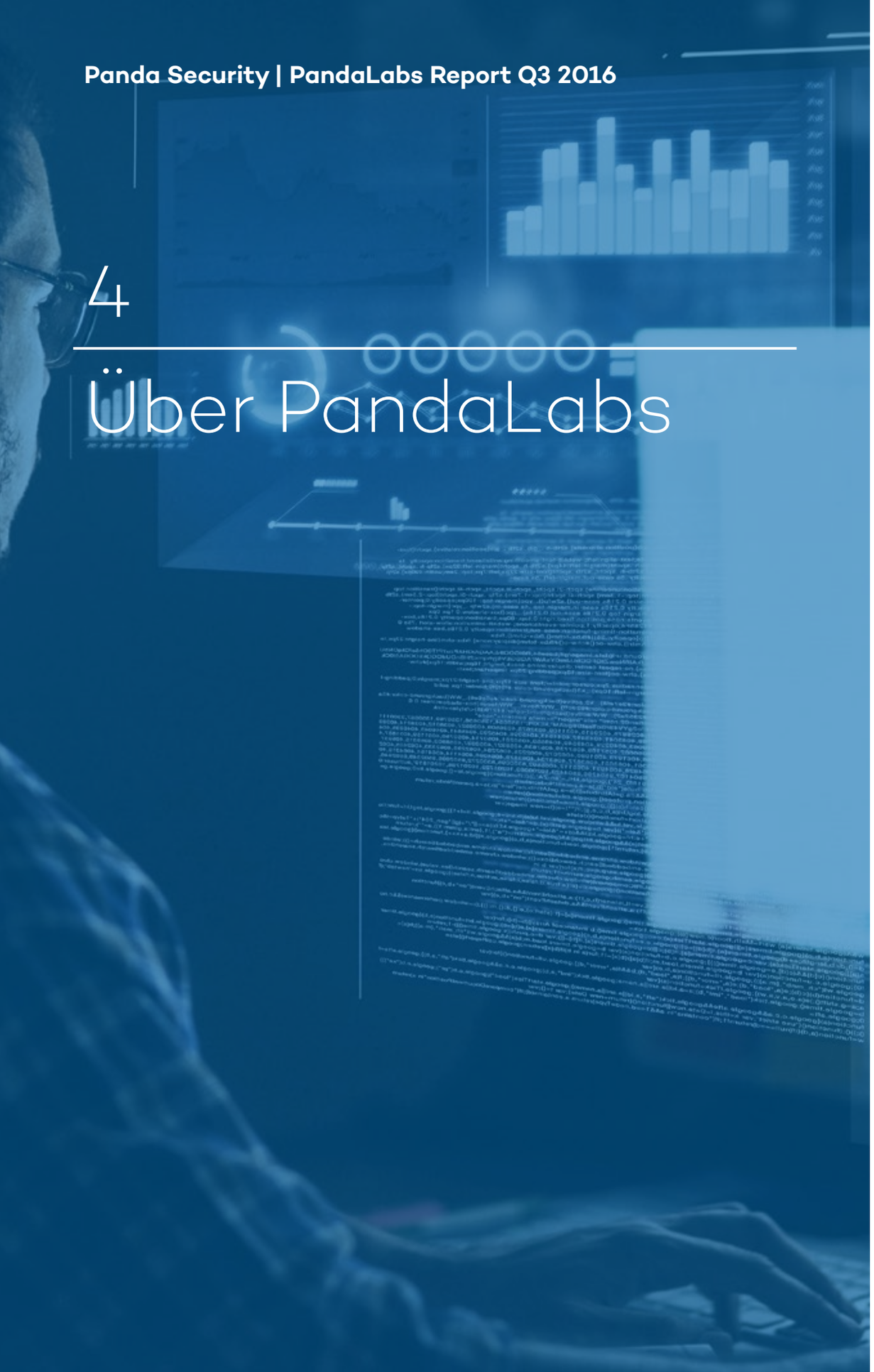
3. FAZIT

3 Fazit

Das Jahr 2016 neigt sich dem Ende zu und **wir müssen unsere Aufmerksamkeit weiterhin der Entwicklung von DDoS-Attacken widmen.** Die Kombination von Millionen von hackbaren IoT-Geräten und die zunehmend schnelleren Internetverbindungen, die wir zu Hause haben, könnten diese Angriffe zu einem der größten Internet-Alpträume machen. Sie haben das Potenzial, jeden zu treffen, insbesondere Unternehmen, die von professionellen Erpressern ins Visier genommen werden.

Datendiebstahl nimmt weiterhin zu und hat das zweite Quartal bereits übertroffen. Im dritten Quartal wurden die Daten von 500 Millionen Yahoo-Nutzern gestohlen. Schutzmaßnahmen zu ergreifen, ist wichtiger denn je: Vergessen Sie nie die Zwei-Faktor-Authentifizierung, wenn Sie sich bei Internetdiensten anmelden. Sie wird verhindern, dass Ihr Account gehackt wird, auch wenn Ihre Anmeldedaten gestohlen oder weitergegeben werden.

4. ÜBER PANDALABS



4 Über PandaLabs

PandaLabs ist Panda Securitys Anti-Malware-Labor und stellt das Nervenzentrum des Unternehmens für Malware-Behandlung dar:

- PandaLabs entwickelt ständig und in Echtzeit die notwendigen Gegenmaßnahmen, um weltweit Panda-Security-Kunden vor allen Arten von schädlichem Code zu schützen.
- PandaLabs ist somit verantwortlich für die Durchführung detaillierter Scans von allen Arten von Malware, mit dem Ziel, den Schutz für Panda-Security-Kunden zu verbessern und die allgemeine Öffentlichkeit zu informieren.

Bei PandaLabs ist man ständig wachsam und beobachtet genau die verschiedenen Trends und Entwicklungen, die im Bereich Malware und Sicherheit stattfinden.

Ziel ist es, sowohl vor drohenden Gefahren und Bedrohungen zu warnen, als auch zukünftige Ereignisse vorherzusagen.

pandalabs

panda

pandalabs