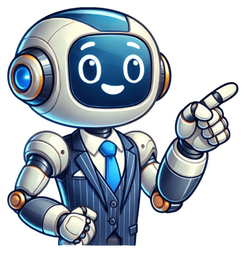
Click Here



So sind die CIA-Experten den Dokumenten zufolge auch im Generalkonsulat der USA in Frankfurt am Main tätig . Dort, in der Gießener Straße, befindet sich das größte US-Konsulat weltweit. Es beherbergt laut WikiLeaks-Dokumenten auf seinem Gelände eine "Sensitive Compartmented Information Facility" (SCIF), ein Gebäude, das nur Mitarbeitern der CIA und anderer US-Geheimdienste zugänglich ist. Diese Digitalspione arbeiten offenbar voneinander abgeschottet "undercover" in der Einrichtung.Für die Dienstreisen dieser CIA-Experten nach Frankfurt gibt es in den Dokumenten Hinweise, gespickt mit einem spezifischen Geheimdiensthumor: "Flying Lufthansa: Booze is free so enjoy (within reason)", heißt es da, also: "Alkohol ist umsonst, also genieße (aber in Maßen)." Dazu gibt es Hinweise fürs Verhalten in den empfohlenen Hotels: "Do not leave anything electronic or sensitive unattended in your room. (Paranoid, yes but better safe than sorry.)" Auch wenn es paranoid klinge, sollten die Mitarbeiter keine elektronischen Geräte oder Vertrauliches unbeaufsichtigt in ihrem Zimmer lassen. Ein früherer Mitarbeiter des US-Geheimdienstes CIA soll wegen Weitergabe geheimer Dokumente an die Enthüllungsplattform WikiLeaks mehrere Jahrzehnte ins Gefängnis. US-Medien berichteten unter Berufung auf das US-Verteidigungsministerium, der 35-jährige Programmierer Joshua Schulte sei wegen Spionage und des Besitzes von Missbrauchsdarstellungen von Kindern zu 40 Jahren Gefängnis verurteilt worden. USA Schulte ist nach Angaben der US-Behörden für den größten Diebstahl geheimer Daten in der Geschichte der CIA verantwortlich. Die CIA sprach, in Anlehnung an den japanischen Großangriff auf den US-Marinestützpunkt Pearl Harbor im Zweiten Weltkrieg, von einem "digitalen Pearl Harbor". Schulte hatte zwischen 2012 und 2016 für ein Hacker-Team der CIA gearbeitet. Er sammelte dabei vom US-Auslandsgeheimdienst eingesetzte Schadsoftware zur Cyberspionage und gab sie später an WikiLeaks weiter. Im März 2017 veröffentlichte WikiLeaks Tausende Seiten von vertraulichen Dokumenten. Daraus ging hervor, dass die CIA eine eigene Programmiertruppe aufgebaut hatte, um durch Schwachstellen unter anderem in Smartphones, Computern und Fernsehgeräten Verdächtige gezielt auszuspähen. Die Enthüllungsplattform veröffentlichte die entsprechenden Dokumente unter dem Namen "Vault 7". Damit erhielten Hacker weltweit Zugriff auf diese Werkzeuge. Schulte soll aus Wut über frühere Kollegen gehandelt haben. "Schamloseste und abscheulichste Spionageverbrechen" "Schulte hat sein Land verraten, indem er einige der schamlosesten und abscheulichsten Spionageverbrechen in der US-Geschichte begangen hat", teilte die Staatsanwaltschaft mit. Der Diebstahl und die Veröffentlichung der Programme hätten den Fähigkeiten der CIA, Geheiminformationen über Gegner der USA zu sammeln, "sofort und schwer geschadet". Mitarbeiter und Programme der CIA seien einem Risiko ausgesetzt gewesen, das Datenleck habe den Geheimdienst "Hunderte Millionen von Dollar" gekostet. Newsletter Starten Sie mit unserem kurzen Nachrichten-Newsletter in den Tag. Erhalten Sie zudem freitags den US-Sonderletter "Was jetzt, America?" sowie das digitale Magazin ZEIT am Wochenende. Mit Ihrer Registrierung nehmen Sie die Datenschutzerklärung zur Kenntnis. Prüfen Sie Ihr Postfach und bestätigen Sie das Newsletter-Abonnement. Schulte war 2017 zunächst nur wegen des Besitzes von Missbrauchsdarstellungen von Kindern angeklagt worden. Die Vorwürfe wegen des Diebstahls und der Weitergabe von Informationen zur nationalen Sicherheit der USA kamen später hinzu. Er wurde 2020 wegen Falschaussage und Missachtung des Gerichts verurteilt und 2022 wegen Spionage- und Hacker-Vorwürfen schuldig gesprochen. 2023 kam eine Verurteilung wegen des Besitzes von Missbrauchsdarstellungen hinzu. Nun wurde das Strafmaß verkündet. WikiLeaks hat mehr als 8700 Dokumente veröffentlicht, die aus dem Cyber-Intelligence-Zentrum des US-Geheimdienstes CIA stammen sollen. WikiLeaks vs. CIA: Wir sagen Ihnen, was Sie zum Thema wissen müssen. Foto: MyImages-Micha – shutterstock.comDas hat Wikileaks veröffentlichtDarunter befinden sich offensichtlich mehr als 24 einsatzbereite und bisher nicht bekannte Cyber-Waffen – unter anderem für den Angriff auf Android-Systeme. Einige davon wurden – wie den Dokumenten zu entnehmen ist – von der CIA selbst entwickelt. Andere wurden von der NSA, dem britischen Geheimdienst GCHQ und Cyberwaffen- Dealern "zugeliefert". Einige der Hacking-Tools, die gezielt Smartphones ins Visier nehmen und von der CIA entwickelt wurden, befähigen den Geheimdienst die Verschlüsselung von WhatsApp, Confide und anderen Apps zu umgehen. Das funktioniert laut WikiLeaks, indem Gesprächsdaten jeglicher Art abgefangen werden, bevor die Verschlüsselung stattfindet. Die Dokumente zeichnen ein Bild, das Verschwörungstheoretiker schon länger kolportieren: Offenbar hat die CIA Zero-Day-Exploits für verschiedene IT-Systeme "gehortet" – trotz Beteuerungen der Obama-Administration, Informationen über Schwachstellen mit den Herstellern teilen zu wollen. Die Dokumente erstrecken sich über den Zeitraum 2013 bis 2016 und stellen laut WikiLeaks "die bislang größte Veröffentlichung von vertraulichen CIA-Dokumenten" dar. Darüber hinaus zeige die Veröffentlichung nun "das gesamte Leistungsvermögen der CIA in Sachen Hacking" auf. Dabei beziehen sich die geleakten Dokumente keineswegs nur auf Android-Gerätschaften: Der Einsatz von Hacking-Tools und Malware gegen iPhones und Smart TVs wird genauso beschrieben, wie Bemühungen der CIA, Windows OS X, Linux und diverse Router zu kompromittieren. Eine dieser Attacken – Codename "Weeping Angel" – war auf Samsung TVs ausgerichtet und wurde laut den Analysen von WikiLeaks von CIA und MI5 entwickelt. Bei dieser Geheimdienst-Operation wurden die Fernseher in einen "Fake-Off"-Modus versetzt, um das Gerät anschließend unbemerkt zu Abhörzwecken verwenden zu können. Aufgezeichnete Gespräche konnten demnach über das Netz direkt auf die CIA-Server "gestreamt" werden. Das war noch nicht alles: Ende 2014 soll die CIA nach Wegen gesucht haben, die Software-Systeme von Fahrzeugen zu infiltrieren. Von Seiten der CIA wollte man sich zur Authentizität der Dokumente zunächst nicht äußern. Dean Boyd, Director of Public Affairs beim CIA, sagte lediglich: "Julian Assange stellt nicht gerade eine Bastion der Wahrheit und Integrität dar." Darüber hinaus ließ der Geheimdienst verlauten, dass seine Überwachungsaktivitäten ausschließlich auf ausländische Geheimdienste abzielen.Im Nachgang verurteilte die CIA die Veröffentlichung der Dokumente durch WikiLeaks mit Nachdruck: "Die amerikanische Öffentlichkeit sollte besorgt sein über Enthüllungen, die für die Fähigkeit der Geheimdienste, Amerika vor Terroristen und anderen Feinden zu schützen, schädlich sein können", schrieb CIA-Sprecherin Heather Fritz Horniak in einer E-Mail. "Solche Enthüllungen setzen nicht nur das Leben von US-Staatsdienern und Geheimoperationen aufs Spiel, sondern statten unsere Feinde mit Werkzeugen und Informationen aus, um uns zu schaden". Das sagt Julian AssangeWikiLeaks-Mastermind Julian Assange äußerte sich im Rahmen einer Pressekonferenz zu den Enthüllungen. In Geheimdienst-Kreisen wurden offensichtlich schon vor der öffentlichen Enthüllung durch WikiLeaks Informationen über angebliche CIA-Cyberangriffe "herumgereicht", wie Assange sagte. "Die CIA hat die Kontrolle über ihr komplettes Arsenal von Cyberwaffen verloren. Es ist ein historischer Akt von vernichtender Inkompetenz, ein solches Arsenal angelegt und es an einem einzigen Ort ungesichert abgespeichert zu haben", so Assange.Über die Quelle, aus der WikiLeaks die Dokumente erhalten hat, wollte sich der Chefredakteur der Enthüllungsplattform freilich nicht äußern. Er ließ aber anklingen, dass die mehr 8700 Dokumente – die angeblich von einem abgeschirmten CIA-Server stammen – über einen Insider zu WikiLeaks gelangten. Aufmerksam wurde die Enthüllungsplattform auf die Dokumente, nachdem diese von mehreren Personen aus dem Umfeld der US-Geheimdienste "auf ungewöhnliche Weise" verbreitet wurden. WikiLeaks, bekräftigte Assange, werde mit den betroffenen Tech-Unternehmen zusammenarbeiten, um die in den geleakten Dokumenten beschriebenen Sicherheitslücken zu schließen. Die Hersteller sind unterdessen bereits tätig geworden: Apple beispielsweise ließ verlauten, man habe bereits die meisten iOS-Schwachstellen beseitigt. Die WikiLeaks-Pressekonferenz mit Julian Assange wurde über Periscope live auf Twitter übertragen. Das sollten Unternehmen tunUnternehmen die wegen der geleakten Dokumente besorgt sind, sollten zu allererst eine Risiko-Einschätzung durchführen, die die neuen Entwicklungen mit einbezieht. Zwar enthalten die geleakten CIA-Dokumente – auch bekannt unter dem Namen "Vault 7" – keinen Schadcode, allerdings werden die verschiedenen Schwachstellen und wie man diese ausnutzt detailliert beschrieben. Sowohl für Security-Fachleute, als auch für potenzielle Angreifer könnten diese Informationen nützlich sein.Die WikiLeaks-Enthüllungen zu den Aktivitäten der CIA zeige deren Möglichkeiten und Ziele, verschaffe aber auch eine breitere Perspektive, wie Michael Shaulov von Check Point Software betont: "Ersetzen Sie CIA einfach durch eine beliebige Institution und Sie haben eine Blaupause davon, wie geschulte Akteure vorgehen". Der nächste Schritt für die IT-Sicherheits-Experten in Unternehmen bestehe nun darin, ihre aktuellen Schutzmaßnahmen dahingehend zu überprüfen, ob diese den in den Dokumenten beschriebenen Bedrohungen standhalten würden: "Sie müssen wissen, wo die Lücken klaffen", so der Experte. Da der Schadcode bislang nicht veröffentlicht wurde, die Schwachstellen aber weiterhin bestehen könnten, sollten Unternehmen nach Meinung von Shaulov auf Tools zur Erkennung von Zero-Day-Angriffen setzen. Wenn die spezifischen Exploits – gemäß der Versprechungen von WikiLeaks – in verantwortungsvoller Weise und in Kooperation mit den Herstellern veröffentlicht werden, sollten die Sicherheits-Experten in Unternehmen sicherstellen, dass gepatcht wird. Angesichts des laxen Patch-Verhaltens in vielen Unternehmen könnten die Exploits aber noch über einen langen Zeitraum zur Anwendung kommen. John Pironti vom Security-Beratungsunternehmen IP Architects gibt unterdessen zu bedenken, dass die Schwachstellen, die in den "Vault 7"-Dokumenten beschrieben werden, von findigen (kriminellen) Hackern "nachgebaut", beziehungsweise zur Schaffung neuer Bedrohungsarten verwendet werden könnten: "Diese Details sind wie Brotkrumen, die zu vielversprechenden Schlupflöchern führen. Die Zeit, die Cyberkriminelle sonst für die Recherche brauchen, hat sich gerade massiv verkürzt". Abschnittsweise beschäftigen sich die von WikiLeaks veröffentlichten CIA-Dokumente auch damit, es den Opfern von Cyberangriffen schwerer zu machen, Gegenmaßnahmen einzuleiten, forensische Maßnahmen durchzuführen und Angriffe zu attribuieren. Diese Informationen könnten insbesondere für weniger erfahrene, kriminelle Hacker nützlich sein, wie Pironti weiß: "Diese Informationen können Anfängern dabei helfen, sich ‚weiterzubilden', während erfahrene Cyberkriminelle hierdurch die Effektivität ihrer Angriffe weiter steigern könnten."Dieser Artikel basiert in Teilen auf einem Beitrag unserer US-Schwesterpublikation networkworld.com. Mit Material von IDG News Service.Glauben Sie … Foto: Brian A Jackson – shutterstock.com… an die Möglichkeit, ihre Systeme gründlichst verteidigen zu können und versuchen Sie daher, alles dafür zu tun, alle Bereiche des Unternehmens jeden Tag ein bisschen besser zu schützen?Schauen Sie … Foto: STILLFX – shutterstock.com… sich nach neuen Instrumenten um, die Funktionsumfang und -tiefe der bestehenden Security-Werkzeuge verbessern?Überwachen Sie … Foto: chombosan – shutterstock.com… alle Sensoren Ihres Netzes – sowohl visuell als auch mit technischen Mitteln?Suchen Sie … Foto: holbox – shutterstock.com… kontinuierlich nach neuen Wegen, um Sensordaten besser zu untersuchen und zueinander in Beziehung setzen zu können?Widmen Sie … Foto: Olivier Le Moal – shutterstock.com… der Sicherheit Ihrer geschäftskritischen Anwendungen samt der dort verarbeiteten vertraulichen Daten erhöhte Aufmerksamkeit?Versuchen Sie … Foto: docstockmedia – shutterstock.com… Tag für Tag, Ihr Business besser zu verstehen, damit Sie die IT-Risikoanalyse dem anpassen und stetig verbessern können?Behalten Sie … Foto: JunPhoto – shutterstock.com… Ihre Zulieferer im Blick, damit der Zugriff von Dritten auf vertrauliche und sensible Daten kontrolliert werden kann?Arbeiten Sie … Foto: totojang1977 – shutterstock.com… eng mit den Geschäftsentscheidern zusammen, um die Aufmerksamkeit für das Thema IT-Sicherheit konstant hoch zu halten und über das gesamte Unternehmen hinweg eine Awareness zu erzeugen?Bewegen Sie … Foto: Lightspring – shutterstock.com… sich in neuen Geschäftsfeldern, in denen disruptive Technologien zum Einsatz kommen und in denen Sie Ihr Security-Wirken schon entfalten können, bevor es richtig ernst wird?Verlieren Sie … Foto: ChristianChan – shutterstock.com… nie die Security-Grundlagen aus den Augen – wie beispielsweise das regelmäßige Patchen? 15 June, 2017 Today, June 15th 2017, WikiLeaks publishes documents from the CherryBlossom project of the CIA that was developed and implemented with the help of the US nonprofit Stanford Research Institute (SRI International). CherryBlossom provides a means of monitoring the Internet activity of and performing software exploits on Targets of interest. In particular, CherryBlossom is focused on compromising wireless networking devices, such as wireless routers and access points (APs), to achieve these goals. Such Wi-Fi devices are commonly used as part of the Internet infrastructure in private homes, public spaces (bars, hotels or airports), small and medium sized companies as well as enterprise offices. Therefore these devices are the ideal spot for "Man-In-The-Middle" attacks, as they can easily monitor, control and manipulate the Internet traffic of connected users. By altering the data stream between the user and Internet services, the infected device can inject malicious content into the stream to exploit vulnerabilities in applications or the operating system on the computer of the targeted user. The wireless device itself is compromized by implanting a customized CherryBlossom firmware on it; some devices allow upgrading their firmware over a wireless link, so no physical access to the device is necessary for a successful infection. Once the new firmware on the device is flashed, the router or access point will become a so-called FlyTrap. A FlyTrap will beacon over the Internet to a Command & Control server referred to as the CherryTree. The beaconed information contains device status and security information that the CherryTree logs to a database. In response to this information, the CherryTree sends a Mission with operator-defined tasking. An operator can use CherryWeb, a browser-based user interface to view Flytrap status and security info, plan Mission tasking, view Mission-related data, and perform system administration tasks. Missions may include tasking on Targets to monitor, actions/exploits to perform on a Target, and instructions on when and how to send the next beacon. Tasks for a Flytrap include (among others) the scan for email addresses, chat usernames, MAC addresses and VoIP numbers in passing network traffic to trigger additional actions, the copying of the full network traffic of a Target, the redirection of a Target's browser (e.g., to Windex for browser exploitation) or the proxying of a Target's network connections. FlyTrap can also setup VPN tunnels to a CherryBlossom-owned VPN server to give an operator access to clients on the Flytrap's WLAN/LAN for further exploitation. When the Flytrap detects a Target, it will send an Alert to the CherryTree and commence any actions/exploits against the Target. The CherryTree logs Alerts to a database, and, potentially distributes Alert information to interested parties (via Catapult). WikiLeaks hat Tausende Dokumente veröffentlicht, die den Cyber-Werkzeugkasten der CIA offenlegen sollen. Was bedeutet das für Nutzer? Kann der Geheimdienst damit auch WhatsApp knacken? Antworten auf die wichtigen Fragen. Zeichen der amerikanischen Central Intelligence Agency (Archivbild) Foto: Carolyn Kaster/ dpa Dieser Beitrag stammt aus dem SPIEGEL-Archiv. Warum ist das wichtig? Am Ende dieses Textes steht ein Update. Der US-Geheimdienst Central Intelligence Agency (CIA) ist offenbar schon seit Längerem dabei, sich seine "eigene NSA" aufzubauen: Diese Botschaft vermittelt zumindest WikiLeaks mit seinen neuesten Enthüllungen. Am Dienstag stellte das Enthüllungsportal von Julian Assange Tausende interne, teils geheime Dokumente der CIA online. Hier beantworten wir die wichtigsten Fragen zu dem neuen Leak. 1. Worum geht es in den Dokumenten? Das WikiLeaks-Material dreht sich um mutmaßliche Spionage-Praktiken der CIA. Im ersten Schwung des Leaks mit dem Namen "Vault 7", über die auch der SPIEGEL berichtete, geben knapp 9000 Dokumente und Dateien einen Überblick über das CIA-Repertoire an Cyberwaffen. Zu diesem Repertoire gehört Schadsoftware wie Viren und Trojaner. Außerdem soll die CIA gezielt noch offene Schwachstellen in Systemen ausnutzen, sogenannte Zero-Day-Exploits. Die Dokumente legen nahe, dass die CIA iPhones von Apple, Android-Geräte von Google, Windows-Rechner und auch mit dem Internet vernetzte Fernseher angreift. So soll etwa der Samsung-Smart-TV F8000 von der CIA in einen Zustand des "Fake Off" versetzt werden können. Der Besitzer denkt dann, das Gerät sei ausgeschaltet, heißt es. Die CIA kontrolliere in der Operation mit dem Codenamen "Weeping Angel" aber das Mikrofon und die Webcam des TV-Geräts. Weitere Dokumente deuten darauf hin , dass die CIA die Steuerung von vernetzten Autos übernehmen könnte. So könnte der Geheimdienst nach Spekulationen von WikiLeaks schwer aufzuklärende Mordanschläge verüben. Ob er die nötigen Kapazitäten für einen solchen Angriff aber wirklich erreicht hat, lassen die Dokumente offen.Die CIA spioniert offenbar zudem nicht nur aus den USA. Hacker des Dienstes sind gemäß den Enthüllungen auch im amerikanischen Generalkonsulat in Frankfurt am Main tätig . Es beherbergt laut WikiLeaks-Dokumenten auf seinem Gelände eine "Sensitive Compartmented Information Facility" (SCIF) - einen Gebäudeteil, der nur Mitarbeitern der CIA und anderer US-Geheimdienste zugänglich ist. 2. Was heißt das für mich als Nutzer? Stimmen die Informationen aus den Dokumenten, hat die CIA offenbar weitreichende Möglichkeiten, technische Geräte von Zielpersonen anzugreifen. Für Beunruhigung dürfte vor allem die Behauptung sorgen, dass es der CIA angeblich gelungen ist, die Verschlüsselung von Messengerdiensten wie WhatsApp, Signal oder Telegram zu umgehen. Das bedeutet aber nicht zwangsläufig, dass die Verschlüsselung, die etwa WhatsApp letztes Jahr eingeführt hat, geknackt werden kann. Das betonte der Krypto-Spezialist Open Whisper Systems, der die technische Basis für die Sicherheit von Kommunikations-Apps wie WhatsApp und Signal liefert. Die Verschlüsselung an sich hält die Firma weiter für sicher. Vielmehr gehe es in den beschriebenen Szenarien darum, die Software der Telefone zu hacken. Auf diesem Weg könnten dann Informationen vor der Verschlüsselung oder nach der Entschlüsselung abgegriffen werden - weil der Angreifer sich Zugriff auf die Geräte verschaffen konnte. WhatsApp oder Telegram als App-Anbieter können gegen solche Angriffe nichts machen: Hier wären etwa Apple und Google gefragt, ihre Systeme zu schützen.Nutzer stehen aber zumindest in der Verantwortung, ihre Betriebssysteme und Apps aktuell zu halten. Wer etwa eine veraltete Android-Version benutzt, in der Sicherheitslücken nicht mehr geschlossen werden, ist ein leichtes Ziel für Angreifer.Gegen Geheimdienste-Angriffe, die auf Zero-Day-Exploits in den Betriebssystemen basieren, kann man sich dagegen schwer schützen. Immerhin ist das Ausnutzen solcher Lücken meist mit größerem Aufwand verbunden. Weil das Risiko einer Entdeckung bei massenhafter Ausnutzung steigt, ist davon auszugehen, dass auch die CIA im Zweifelsfall eher auf zielgerichtete Attacken auf einzelne Personen setzt. 3. Was weiß man über die Hintergründe der Veröffentlichung? Eine anonyme Quelle soll WikiLeaks das Material zugespielt haben. Laut WikiLeaks kursierten die Dokumente unter US-Regierungshackern und Zulieferfirmen und sollen aus diesen Kreisen zur Enthüllungsplattform gelangt sein.Nach eigenen Angaben haben die Mitarbeiter der Organisation die Dokumente mehrere Monate lang durchgearbeitet und vor der Veröffentlichung bestimmte Stellen geschwärzt - zum Beispiel die Klarnamen von CIA-Mitarbeitern, ihre E-Mail-Adressen oder die IP-Adressen ihrer Rechner.In der Vergangenheit hatte es immer wieder Kritik an WikiLeaks gegeben, weil die Plattform große Mengen unbearbeiteter Dokumente online gestellt hatte. Dass WikiLeaks diese umstrittene Arbeitsweise nun offenbar angepasst hat, ging im Zuge der Enthüllungen fast ein wenig unter. Unter anderem wies aber der Journalist Glenn Greenwald, der selbst mit den Snowden-Dokumenten über die NSA gearbeitet hatte, auf diesen Umstand hin . 4. Welche Reaktionen gab es auf die Enthüllungen? Die CIA kommentierte die WikiLeaks-Veröffentlichung nur knapp. "Wir äußern uns nicht zur Authentizität oder den Inhalt von angeblichen Geheimdienst-Dokumenten", sagte ein Sprecher auf eine Anfrage der Nachrichtenagentur dpa. Auch der Sprecher von US-Präsident Donald Trump, Sean Spicer, wollte das Leak nicht kommentieren.Ein Sprecher der Bundesregierung sagte dem SPIEGEL auf Anfrage, man äußere sich zu nachrichtendienstlichen Angelegenheiten "grundsätzlich nur gegenüber den zuständigen, geheim tagenden Gremien des Deutschen Bundestages." Ein Sprecher des Außenministeriums sagte laut der Nachrichtenagentur Reuters, man stehe in engem Kontakt mit den US-Behörden. Auch der deutsche Generalbundesanwalt will sich laut einem Sprecher das Leak ansehen und Ermittlungen einleiten, sollten sich konkrete Hinweise auf Fehlverhalten finden. Von Samsung, deren Fernsehgerät in den Leaks auftaucht, hieß es auf Anfrage des SPIEGEL, der Schutz der Kundenprivatsphäre habe für die Firma einen sehr hohen Stellenwert. Man prüfe die aktuellen Berichte "mit höchster Dringlichkeit".Ein Apple-Sprecher sagte dem US-Portal "TechCrunch" , dass "viele" der in den Leaks genannten Schwachstellen durch seine Firma bereits behoben seien: "Wir werden weiter daran arbeiten, alle entdeckten Schwachstellen schnell zu schließen." Update, 9. März: Mittlerweile gibt es auch eine Stellungnahme von Google. Laut "Recode" heißt es vom Konzern , man sei zuversichtlich, dass Sicherheits-Updates und Schutzmaßnahmen in Chrome und Android die Nutzer bereits vor den mutmaßlichen Bedrohungen schützen. Auch Samsung hat seine erste Stellungnahme konkretisiert. Betroffen von dem Angriff sei Firmware von Fernsehern, die 2012 und 2013 auf den Markt gebracht wurden. Bei einem Großteil der betroffenen Geräte wurde die Schwachstelle laut Samsung bereits über ein Update behoben. Zudem funktioniert der Angriff laut Samsung nur, wenn Angreifer physischen Zugang zum TV hatten, um per USB-Stick Schadsoftware zu übertragen. Logo für die Dokumente mit der Sammelbezeichnung Vault 7 Vault 7 ist eine Reihe von Dokumenten, die WikiLeaks ab März 2017 über einen Zeitraum von sechs Monaten veröffentlichte. Die Dokumente beschreiben detailliert die Aktivitäten und Fähigkeiten der Central Intelligence Agency (CIA) der Vereinigten Staaten zur Cyber-Kriegsführung und zur Durchführung von elektronischer Überwachung. Die Dateien, die von 2013 bis 2016 datiert sind, enthalten Details zu den Softwarefunktionen der CIA, wie z. B. die Möglichkeit, Autos, Smart-TVs, Webbrowser (einschließlich Google Chrome, Microsoft Edge, Mozilla Firefox und Opera), und die Betriebssysteme der meisten Smartphones (einschließlich Apple iOS und Google Android) sowie andere Betriebssysteme wie Microsoft Windows, macOS und Linux zu kompromittieren.[1] Die CIA zeigte sich besorgt über die Veröffentlichungen,[2] ging aber von der Echtheit der veröffentlichten Dokumente aus. Im Juni 2018 wurde der ehemalige CIA-Mitarbeiter Joshua Adam Schulte angeklagt, die geheimen Dokumente an Wikileaks weitergeleitet zu haben.[3] Nach der Veröffentlichung von Vault 7 erwog die CIA, den WikiLeaks-Gründer Julian Assange zu entführen und zu töten.[4][5] Joshua Schulte wurde von einem Bundesgericht in New York am 1. Februar 2024 zu 40 Jahren Gefängnis verurteilt.[6] Von den 40 Jahren Haft entfallen aber 6 Jahre und acht Monate auf eine Verurteilung wegen Besitzes von Kinderpornografie, die nach Angaben der Behörden auf Schultes Computer gefunden wurde. In einer anschließenden Erklärung sagte US-Staatsanwalt Damian Williams, Schulte habe „sein Land verraten, indem er einige der dreistesten, abscheulichsten Spionageverbrechen in der amerikanischen Geschichte begangen hat".[7] Der ursprüngliche Prozess gegen Schulte im Jahr 2020 endete mit einem Fehlverfahren, da sich die Geschworenen bei den schwerwiegendsten Anklagepunkten uneinig waren. Im Juli 2022 wurde er jedoch in einem weiteren Prozess im Zusammenhang mit der Verschlusssache verurteilt.[8] Homepage von Wikileaks Vault 7: CIA Hacking Tools Revealed In: Wikileaks, abgerufen am 15. Mai 2019 ↑ WikiLeaks-Enthüllung: So kann die CIA angeblich auf Apple-Laptops zugreifen. In: Spiegel Online. 23. März 2017 (spiegel.de [abgerufen am 15. April 2019]). ↑ heise online: Vault 7: CIA ist sauer auf Wikileaks. Abgerufen am 15. April 2019. ↑ WikiLeaks-Enthüllungen "Vault 7": Anklage gegen Ex-CIA-Mitarbeiter. Spiegel Online, 19. Juni 2018, abgerufen am 4. Dezember 2019. ↑ Julian Assange: CIA soll Bericht zufolge Ermordung des WikiLeaks-Gründers erwogen haben. In: Der Spiegel. 28. September 2021, ISSN 2195-1349 (spiegel.de [abgerufen am 28. September 2021]). ↑ netzpolitik.org Julian Assange – Die Rache der CIA ↑ Hacker-Programme an Wikileaks: Ex-CIA-Mitarbeiter zu 40 Jahren Haft verurteilt. 2. Februar 2024, abgerufen am 5. Februar 2024. ↑ Former CIA engineer who sent 'Vault 7' secrets to Wikileaks sentenced to 40 years. 2. Februar 2024, abgerufen am 5. Februar 2024 (englisch). ↑ This ex-CIA computer Vault 7 hacker gave secrets to WikiLeaks. 4. Februar 2024, abgerufen am 5. Februar 2024 (englisch). Abgerufen von „ Als „Vault 7" hatte Wikileaks CIA-Programme veröffentlicht, mit denen der Geheimdienst auch auf Handys oder Smart-TVs zugreifen konnte. Der Geheimnisverräter wurde schnell gefasst, nun steht sein Strafmaß fest.Weil er geheime Hacker-Programme der CIA an die Enthüllungsplattform Wikileaks weitergab, ist ein früherer Mitarbeiter des amerikanischen Auslandsgeheimdienstes zu 40 Jahren Gefängnis verurteilt worden. Ein Bundesrichter in New York verhängte am Donnerstag das Strafmaß gegen den 35 Jahre alten Joshua Schulte wegen Spionage, Hacker-Aktivitäten, Missachtung des Gerichtes, Falschaussagen gegenüber der Bundespolizei FBI und Kinderpornografie.Schulte ist nach Angaben der Behörden für den größten Diebstahl geheimer Daten in der Geschichte der CIA verantwortlich. Die CIA sprach in Anlehnung an den japanischen Großangriff auf den Marinestützpunkt Pearl Harbor im Zweiten Krieg sogar von einem „digitalen Pearl Harbor".Schulte hatte zwischen 2012 und 2016 für ein Hacker-Team der CIA gearbeitet. Er sammelte dabei vom Geheimdienst eingesetzte Schadsoftware zur Cyberspionage und gab sie später an Wikileaks weiter. Die Enthüllungsplattform veröffentlichte die entsprechenden Dokumente, die im Gegensatz zu früheren Veröffentlichungen von Wikileaks teilweise zensiert wurden, im März 2017 unter dem Namen „Vault 7".Schulte soll aus Wut darüber gehandelt haben, dass der Geheimdienst in Konflikten mit seinen Kollegen nicht für ihn Partei ergriffen hatte.„Schulte hat sein Land verraten, indem er einige der schamlosesten und abscheulichsten Spionageverbrechen in der amerikanischen Geschichte begangen hat", erklärte die Staatsanwaltschaft. Der Diebstahl und die Veröffentlichung der Programme hätten den Fähigkeiten der CIA, Geheiminformationen über Gegner der Vereinigten Staaten zu sammeln, „sofort und schwer geschadet". Mitarbeiter und Programme der CIA seien einem Risiko ausgesetzt gewesen, das Datenleck habe den Geheimdienst „hunderte Millionen von Dollar" gekostet.Schulte wurde 2017 zunächst wegen des Besitzes von Kinderpornografie angeklagt. Bei den Ermittlungen wurden auf seinen Computern entsprechende Daten gefunden worden. Die Vorwürfe wegen des Diebstahls und der Weitergabe von Informationen zur nationalen Sicherheit der Vereinigten Staaten kamen später hinzu.Zur Startseite

- tego
- https://isleo.com/i_photos/file/e9648435-938e-4d65-bdeb-13c9207d3543.pdf
- what is a primate city gcse geography
- https://baohohoanglong.com/userfiles/file/gefomafikipiju.pdf
- hororabu
- http://borui-cn.com/img/files/wineg-rozedutesajolof-zixerenorabeti-fuduwezaxupovu.pdf
- juyaro
- download windows 10 1803 iso file
- reyaxuha
- motivational interviewing example questions
- zecibiba
- https://ijestr.com/ckfinder/userfiles/files/f2981794-7996-4716-9e81-1fbd5bb1965c.pdf
- do simplicity sewing patterns include seam allowance
- how to install gta 4 on windows 7 32-bit
- https://nhaccugiare24h.com/uploads/userfiles/file/tuzigasebe.pdf
- http://pccctananhdung.com/upload/files/7b2fb262-61b4-4a31-8fa7-f61dac042145.pdf
- http://kubabus.cz/novy-web/upload/file/49918091738.pdf
- chapter 7 fair game review answer key
- xipasovulo