CVE 2022 41328 Fortinet Zero Day exploitation

Abstract:

Diese Arbeit untersucht ein kritischen und komplexen Cyberangriff auf Fortinet, einem führenden IT-Sicherheitsunternehmen.
Angesichts der Tatsache, dass staatliche Akteure zunehmend Cyberangriffe unterstützen oder durchführen und dabei ausgefeilte Taktiken anwenden, ist dies von entscheidender Bedeutung für die heutige Zeit.

Die Analyse konzentriert sich auf die Ausnutzung von CVE-2022-41328, einer hochrangigen Schwachstelle in der FortiGate Firewall von Fortinet. Darüber hinaus wird die Manipulation des Python-basierten Web-Frameworks Django untersucht, das in den Fortinet-Systemen FortiManager und FortiAnalyzer zum Einsatz kommt., um eine erweiterte Systemkontrolle und Verbindungen zu einem Kommandoserver zu ermöglichen. Der Bericht zeigt, wie es den Angreifern gelungen ist, in drei der Fortinet Produkte einzudringen und die höchsten Privilegien auf den Systemen zu erlangen.

Dies unterstreicht die entscheidende und auch wachsende Relevanz der IT-Sicherheit in der heutigen digitalen Welt. Insbesondere im Zusammenhang mit staatlich unterstützten Cyberangriffen, die eine wachsende Bedrohung für Unternehmen und Regierungen auf der ganzen Welt, Unternehmen, die in der IT-Sicherheitsbranche Technologien vertreiben und damit für die Sicherheit dritter verantwortlich sind oder jene, die mit sensiblen Daten von Benutzern, Staaten oder Firmen arbeiten, die unter keinen Umständen in die Hände von Dritten kommen sollten.

Darüber hinaus wird eine Verbesserung der Reaktion auf solche Angriffe, sowie einer kontinuierlichen Verbesserung der IT-Sicherheitstechnologien und -techniken sowohl in den Systemen als auch den Mitarbeitern beschrieben. Es wird deutlich, dass die Bedrohung durch hoch entwickelte und staatlich unterstützte Cyberangriffe ein zunehmend kritisches Thema ist, dass ein hohes Maß an Sensibilisierung und robuste Sicherheitsmaßnahmen erfordert, die zusammen mit immer komplexeren Angriffen immer höhere Resilienz gegenüber diesen Aufzeigen müssen.

Inhalt

Einleitung

Mit dem stetigen Voranschreiten der Digitalisierung großer und auch kleiner Unternehmen und vieler privater Haushalte wird die IT-Sicherheit immer wichtiger, da ein immer größer werdender Teil unseres Lebens und unserer Informationen digital gespeichert und verarbeitet werden.
Daher investieren immer mehr Firmen enorm in Sicherheitslösungen verschiedenster Anbieter, um ihre Sicherheit und ihre Resilienz gegenüber Angriffen von innen und außen zu verbessern. So wird von dem Marktforschungsunternehmen Gartner Inc. ein Anstieg der globalen Ausgaben in die IT-Sicherheit von 11,3 % für das Jahr 2023 prognostiziert. Das ist ein absoluter Anstieg von über 30 Milliarden US-Dollar im Vergleich zu 2021[0].
Durch die große Verbreitung von externen und standardisierten Sicherheitslösungen werden diese zum Ziel von Angreifern, vor allem von sehr gut finanzierten Akteuren wie Staaten bzw. staatlich finanzierten Organisationen. Diese sind im seltensten Fall an Privatpersonen interessiert, Ihnen geht es um kritische Informationen von Firmen oder NGOs, die dem angreifenden Staat ein Vorteil im globalen Wettrennen oder in der Kontrolle von Organisationen oder Gruppen im eigenen Land ermöglicht[1].

Genau diesen Trend konnte man in den letzten Jahren verfolgen. Während individuelle Angreifer meist über bekannte Schwachstellen mit einfachen Methoden versuchen, Daten und oder Geld zu erbeuten, verwenden gut finanzierte und ausgebildete Organisationen ausgefeilte Techniken, um Anbieter von Sicherheitssystemen oder Betriebssystemen anzugreifen, um sensible Daten über Techniken oder Personen zu erbeuten. Sehen kann man diesen Trend an Programmen wie Pegasus[2] der NSO-Gruppe oder auch den Angriffen mit WannaCry[3]. Sowohl Pegasus als auch NotPetya, obwohl in der Aufgabe unterschiedlich, sind staatlich unterstütze Programme, die unter Verwendung von Zero-Day-Exploits (Schwachstellen, die seit Tag eins unerkannt im System sind) ihre Aufgabe verrichten.

Diese sehr komplexe Art, mit noch die dagewesenen Schwachstellen in Systemen, sprich Zero-Day-Exploits umzugehen und diese sehr gezielt zu verwenden, konnte man auch bei dem Angriff auf Fortinet beobachten. Dort schafften es die Angreifer über einen einziges mit dem Internet verbundenes Gerät, eine Reihe von weit entwickelten Exploits in das System einzuschleusen, um dann über ein lokalen Zero-Day-Exploit dauerhaften Zugang auf die Systeme eines Fortinet Kunden zu erlangen.

Um in Zukunft diese Art von Angriffen besser verhindern zu können, ist es wichtig aus diesen Lehren zu ziehen und das Denken und Handeln dieser hoch finanzierten Gruppen zu analysieren, um neue Wege zu finden, diese noch früher zu erkennen und an der Reaktion nach einem Angriff innerhalb der Unternehmen weiterzuarbeiten.

---

[0] Gartner. (2022). *Gartner Identifies Three Factors Influencing Growth in Security Spending*.
[1] Microsoft.com. (2022). *Nation state threats | Microsoft Security*.
[2] Marczak, B. (2021). *FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild - The Citizen Lab*.
[3] Cloudflare. (2017). *Was war der WannaCry-Ransomware-Angriff?*

Hauptteil:

2.1 Was ist Fortinet und warum sollte man dieses Unternehmen angreifen?

Um zu verstehen, warum Fortinet überhaupt als interessantes Angriffsziel dienen kann, muss eine Basis geschaffen werden, auf der verstanden wird, was dieses Unternehmen vertreibt und wer seine Kunden sind.
Fortinet ist einer der weltweit führenden Unternehmen im Bereich der Hardware für IT-Sicherheit und bedient mit seinen Produkten eine wachsende Anzahl an Unternehmen unterschiedlichster Größe, von Kleinunternehmen bis hin zu multinationalen Konzernen[4]
So sind verschiedene Banken, aber auch Siemens Schweiz und das Lebensmittelunternehmen Dolé unter den Kunden[5].
Im Jahr 2022 konnten Sie einen Gesamtumsatz von 4,42 Milliarden Dollar erwirtschaften, davon waren 1,78 Milliarden der alleinige Umsatz der Fortinet Produkte[6,7]. Das solch ein Erfolg Konkurrenten und staatliche Akteure auf diese Firma blicken lässt, ist naheliegend. Denn nicht nur könnten von einem Konkurrenzunternehmen etwaige technische Fortschritte durch einen Hack gestohlen werden, sondern könnten auch staatliche Akteure ein Interesse haben, eine zuverlässige Sicherheitslücke in diesen Systemen zu finden, um Ziele effizient angreifen zu können, die mit Fortinet Soft- und Hardware geschützt ist.

In dem im Folgenden beschriebenen Angriff wurden drei Produkte der Firma Fortinet erfolgreich angegriffen. Diese sind ein wichtiger Bestandteil der Produktpalette

FortiGate:
ist eine Hardware Firewall entwickelt von Fortinet, diese Regelt den Datenfluss und überwacht durchfließende Pakete. Diese Hardware gibt es in vielen variablen Größen, grundsätzlich sind aber alle Größen gleich aufgebaut[8]

FortiManager:

Ist eine Verwaltungssoftware, die zusammen mit dem eigenen auf Linux aufgebauten OS, dass das Management der Hardware ermöglicht. FotiManager unterstützt auch verschiedenste Integrationen und Automatisierungsmöglichkeiten[9]

FortiAnalyzer:

Ist ein Log-Analyse Tool der Systemlogs schreibt, diese auswertet und verdächtige Logs an den Manager meldet, damit schnell auf Sicherheitsbedrohungen reagiert werden kann[10]

Zusammen bilden diese drei Produkte einen breiten Schutz gegenüber Angriffen auf Systeme, da die Firewall unzulässige Zugriffe und Verbindungen schnell überprüfen kann und mit dem ForitAnalyzer unerlaubte und ungewöhnliche Geschehnisse an die Verwaltungssoftware gemeldet werden und so Fortinet Kunden schnell auf Bedrohungen reagieren können.

---

[4] Autoren der Wikimedia-Projekte (2016). *Fortinet jüngste Entwicklung*
[5] Fortinet. (2022). Fortinet Global Customers and Case Studies.
[6] Q1 2023 Financial Results. (2023).
[7] Fortinet, Inc. (2022). *Fortinet Reports Fourth Quarter and Full Year 2022 Financial Results | Fortinet, Inc.*
[8] Fortinet. (2022). *Next Generation Firewall (NGFW) – Top-Produkte anzeigen.*
[9] Fortinet. (2022). *Erstklassiges Netzwerkverwaltungs-Softwaresystem & Operations-Tool | FortiManager*.
[10] Fortinet. (2022). *Netzwerkanalyse für große und komplexe Netzwerke | FortiAnalyzer*.

2.2 Überblick über CVE-2022-41328 und dessen Verwendung

Mit dem „Common Vulnerabilities and Exposures“ (CVE) Code 2022-41328 wird eine Schwachstelle in der ForiGate Firewall beschrieben. Diese Schwachstelle hat laut dem US-Amerikanischen „National institute of standards and technology“ (NIST) den „Common Vulnerability Scoring System“ (CVSS) Wert 7.1 von 10 maximalen Punkten[11]. Die sicherheitstechnische Relevanz ist demnach sehr hoch. Der von der NIST mitgelieferte „Attack Vector“ zeigt auch auf, dass die Angriffskomplexität gering, die Vertraulichkeit und die Integrität aber schwer getroffen sind, daher auch der hohe CVSS Wert[11]. Das heißt, dass der Angriff, einmal gefunden, leicht wiederholbar ist. Das Finden der Schwachstellen benötigt aber ein tiefes Verständnis der Fortinet Systeme und womöglich ein gekauftes System, um das Verständnis aufbauen zu können.

Der CVSS-Wert ist auch deshalb nicht höher, da der initiale Zugriff auf die Systeme bereits vorhanden sein muss und nur eine permanente Hintertüre in die FortiGate Systeme über diesen Exploit eingeschleust werden kann.
Sobald dieser initiale Zugriff erfolgt ist, kann ein Angriff auf die FortiGate Firewall erfolgen, der eine durch eine Veränderung des Quellpfades, Zugriff auf sonst nicht öffentliche Dateien ermöglicht, genannt „path traversal“ Angriff.
Bevor dieser Zero-Day ausgenutzt werden kann, benötigt es aber noch weitere Vorbereitung.

Schritt 1: Vorbereitung:

Sowohl das FotiManager und FortiAnalyzer System verwenden für sein Webinterface Django[12] - ein auf Python basiertes Webframework[13]. Durch einen Konfigurationsfehler eines FortiManagers oder FortiAnalyzers, durch einen Kunden, war dieser aus Versehen öffentlich auffindbar. Nach der ersten Verbindung zu dem System konnten dann innerhalb dieser Django Installation Änderungen der urls.py Datei vorgenommen werden. Diese verarbeitet API (Application Programming Interface) Aufrufe auf das Django Framework.
Durch das Hinzufügen einer neuen API-Funktion war es nun möglich durch POST-Anfragen mit der neu eingebauten Funktion zu interagieren. Diese erschaffene Hintertür, nennt Mandiant, ein führendes Unternehmen im Bereich der Gefahrenanalyse für IT-Systeme[14], „Thincrust“. Diese kann über das Hinzufügen von Cookies in POST-Anfragen an die API gesteuert werden. So können drei verschiedene Zustände ausgelöst werden, mit denen man Daten abgreifen, schreiben oder neue Funktionen ausführen kann[15].
Um die Authentifizierung für POST-Anfragen zu umgehen, verwendete die Hintertür eine Funktion innerhalb der Django Installation, die eine Ausnahme hinzufügte und so ohne Login oder Login-Token, Post-Anfragen an den Server gesendet und von diesem verarbeitet wurden.
Da der Zugriff auf den FortiManager oder FortiAnalyzer aber nicht genug ist, um Dateien in der Firewall zu verändern und damit weiter in das System vorzudringen, benötigten die Angreifer einen Zugriff auf die FortiGate Firewall

[11] Nist.gov. (2022). *NVD - CVE-2022-41328*.
[12] Mandiant.com. (2023).
[13] Django Project. (2023). *Django overview*.
[14] Mandiant. (2021). *Threat Intelligence & Cyber Security Company | Mandiant | EN*.
[15] Mandiant.com. (2023).

Schritt 2: Verwendung von CVE-2022-41328

Der nächste Schritt war nun, mit dem vorhandenen ersten Zugriff auf das System weiter in das System vorzustoßen, um weitere Daten abgreifen zu können und Privilegien zu erweitern. Dazu verwendeten die Angreifer die path traversal Schwachstelle in der FortiGate Firewall. Diese ermöglichte es über eine schlecht implementierte Upload Methode beliebige Daten, auch solche, die sonst nicht bearbeitet werden dürfen, zu überschreiben[16].
Diese Upload-Methode war sonst nur dazu da Icons über das FTP (File Transfer Protocol) auf FortiGuard hochzuladen, daher wurde innerhalb der Funktion nur geprüft, ob die Dateigröße kleiner als 65 Kilobyte war, nicht aber den Dateityp oder den Speicherort. Genug, um beliebige Skripte hochladen zu können, die noch tieferen Zugriff auf die FortiGuard Systeme zulassen[16]. Dadurch, dass die Dateien für das System über diese Schwachstelle in das System geschrieben werden, wurde die Veränderung der Dateien nicht von dem Logsystem erfasst und in die Logdateien geschrieben. Daher blieb der Angriff so lange unbekannt, bis durch die Schwachstelle Dateien ausgetauscht wurden, die sehr genau überwacht wurden.

2.3 Mit CVE-2022-41328 zu CASTLETAP

Durch die neu gewonnene Möglichkeit Dateien dort zu platzieren, wo man sie haben möchte, konnten die Angreifer nun eine passive Hintertür in der FortiGate Firewall platzieren. Diese konnte, sofern einmal aktiviert, spezielle ICMP („Internet Control Message Protocol“) Pakete abfangen, und dadurch gesteuert werden. Diese wurden von einem eigens von CASTLETAP erstellen Netzwerksockel gelesen und verarbeitet.
Durch Rechnen mit XOR, mit den speziellen ICMP-Paketen konnte dann dir Hintertür gesteuert werden. Wenn das Ergebnis dieser Rechnung eines von zwei fest codierten Strings repräsentierte, konnte entweder der Dienst gestoppt oder weitere Informationen des ICMP-Paketes ausgelesen und danach zu einem Kontrollserver (Command and Control Server) verbunden werden[16].
Nachdem diese Verbindung aufgebaut wurde, kann CASTLETAP Dateien herunter- und hochladen oder eine Shell öffnen, um weitere Kommandos ausführen zu können.

Durch diesen Dienst kann dann auf weitere Systeme zugegriffen werden und weitere Rechte erlangt werden. So beschreibt Mandiant, in einem weiteren Artikel, wie über weitere Schwachstellen, VIRTUALPITA und VIRTUALPIE[17] ein unerlaubter Zugriff auf VMware Dienste möglich ist, worüber es einem Angreifer möglich wäre auf alle virtualisierten Rechner zuzugreifen.

[16]Mandiant. (2022). *Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation | Mandiant*. [online] Available at: https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem [Accessed 14 Jun. 2023].
[17]Mandiant. (2022). *Bad VIB(E)s Part Two: Detection and Hardening within ESXi Hypervisors | Mandiant*. [online] Available at: https://www.mandiant.com/resources/blog/esxi-hypervisors-detection-hardening [Accessed 14 Jun. 2023].

2.4 Zugriff trotz Gegenmaßnahmen

Nachdem die Sicherheitsexperten von Fortinet ungewöhnliche Aktivitäten auf ihren Systemen beobachtet hatten, aktivierten sie auf dem FortiManager eine Access Control List (ACL), die eingehende externe Pakete auf einen einzigen Port beschränkte. Dadurch verloren die Angreifer zunächst den Zugriff auf die Systeme, da der Zugang über die Hintertür CASTLETAP keine Pakete mehr empfangen konnte[16].

Um diese Sperre zu umgehen, mussten die Angreifer nun einige neue Dienste auf den FortiGuard-Systemen installieren. Dazu nutzten sie die bereits gefundene „Path Traversal"-Schwachstelle. Den neu hochgeladenen Dienst nennt Mandiant „TABLEFLIP". Er ist ein passiver Umleitungsdienst, der Datenpakete auf den per ACL erlaubten Port 541 umleiten und so wieder direkten Zugriff auf das FortiGate-System ermöglichen kann[16]. Einmal aktiviert, konnte der Angreifer die TABLEFLIP-Umleitung durch eine bestimmte Zahlenfolge am Anfang eines TCP (Transmission Control Protocol) Datenpakets aktivieren oder deaktivieren[16]. Auch hier wurde die Entschlüsselung der IP und des Ports innerhalb des Datenpaketes über eine XOR-Rechnung mit einer bestimmten Folgen an Buchstaben und Zahlen umgesetzt.

Wurde die Umleitung aktiviert, fügte CASTLETAP eine neue Regel in die Firewall, genauer gesagt in die iptable-Regeln, des FortiGate-Systems ein, die dann den Datenverkehr umleitete. Die Umleitung wurde in den iptable-Regeln in die Prerouting-Kette geschrieben. Diese ist dazu da eingehende Datenpakete direkt zu verarbeiten und konnte damit die ACL-Regeln umgehen. Dadurch war der Zugriff auf das System wieder uneingeschränkt möglich.

Der Angreifer war auch in der Lage, eine hinzugefügte Regel wieder zu löschen, indem er ein spezielles Datenpaket verschickte.
Um wieder Befehle ausführen zu können, installierten die Angreifer eine andere Hintertür, namens REPTILE. Diese ist laut Analysen der Forensiker von Mandiant sehr ähnlich zu einem öffentlich verfügbaren Linux Rootkit.
Auch diese, wie alle anderen davor konnte von eingehenden Paketen gesteuert werden, in dem ein Vergleich mit einem vorher gesetzten String positiv war. Wie bei den Vorgegangenen Hintertüren wurde auch hier entweder der Dienst gestoppt oder weitere Informationen des Datenpaketes ausgelesen und danach zu einem Command and Control Server verbunden werden[16].

[16]Mandiant. (2022). *Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation | Mandiant*. [online] Available at: https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem [Accessed 14 Jun. 2023].

2.5 Versuche den Angriff zu verstecken

Nicht nur war der eigentliche Angriff komplex und vielschichtig, sondern es gab auch viele Maßnahmen, die darauf zielten, den Angriff so lang wie möglich unentdeckt zu halten. So war es zum Beispiel dem Logsystem nicht möglich den initialen Angriff über die CVE 2022-41328 Schwachstelle zu loggen, sofern beim Aufrufen der Funktion keine unerlaubten Dateien überschrieben wurden.
Auch viele der eingeschleusten Programme wurden so installiert, dass der systemeigene FortiGuard Bootmanager diese bei einem Neustart komplett deinstalliert und so Beweise eines Eindringens nur an einem Live-System zu finden sind und nicht mehr, sobald das System einmal neu gestartet wurde. Wenn doch Logs geschrieben wurden, bemühten sich die Angreifer sehr diese Logs auch zu löschen, sodass deutlich weniger Daten in der forensischen Analyse verfügbar waren. So beschreibt Mandiant eine weitere Hintertür in einem FortiGate System, die ein Link zwischen zwei verschiedenen Systemfunktionen herstellt. Durch das Löschen dieser Daten durch den Bootmanager war es den Sicherheitsspezialisten von Fortinet aber unmöglich diese Daten wiederherzustellen und eine forensische Analyse der Daten vorzunehmen.

Zusätzlich deaktivierten die Angreifer ein Verifikationssystem der Bootfiles, um gemachte Änderungen länger verstecken zu können, ohne dass das System ein Fehlen oder eine Änderung der Bootfiles meldet und damit Aufmerksamkeit darauf gelenkt wird.

2.6 Zusammenhang und Herkunft

Mandiant rechnet den Angriff der chinesischen Cyber Spionage Gruppe UNC3886 zu. Diese greift in den letzten Monaten häufig Systeme mit komplexen Zero-Day Schwachstellen an und zeigen dabei in immer tiefer werdendes Verständnis auch von großen und komplexen Systemen. So wurde bereits 2022 ein Zero-Day in Fortinet Produkten von der gleichen Gruppe ausgenutzt[18]. Zusätzlich wurden auch Schwachstellen in VMware Produkten ausgenutzt, die auch dort das Eskalieren von Privilegien bis hin zum vollen administrativen Zugang auf virtualisierten Geräten ermöglichte[19]. Über diese Gruppe ist sonst nur sehr wenig bekannt. So sind weder Mitglieder der Gruppe oder eine klare Zuweisung zu einer Institution bekannt. Fest steht aber, dass die Gruppe sehr gut finanziert und auch ausgebildet sein muss, sonst wäre das Finden dieser Anzahl an Zero-Days und deren Ausnutzung in solch kurzen Abständen in verschiedensten Produkten unterschiedlichster Firmen nicht möglich.

[18]Mandiant. (2022). *Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475) | Mandiant.*
[19]Mandiant. (2022). *Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors | Mandiant.*

Schlussteil

3.1 Learnings

In der immer schneller werdenden Welt der IT-Sicherheit ist es wichtig aus solchen Angriffen Lehren zu ziehen, damit ähnliche Angriffe in Zukunft verhindert werden können. Der Angriff auf Fortinet zeigt die zunehmende Raffinesse und Komplexität von modernen Cyberangriffen. Die Angreifer konnten durch das Ausnutzen neuer Schwachstellen drei Produkte des Unternehmens - FortiGate, FortiManager und FortiAnalyzer - zu kompromittieren. Daraus lässt sich nun eine wichtige Sache lernen. Zuerst dürfen menschliche Fehler, wie das fälschliche Konfigurieren eines Systems, nicht unentdeckt bleiben. Zweitens gewinnt in diesem Kontext die Bedeutung von Lösungen zur Erkennung und Reaktion auf noch unbekannte Bedrohungen an den Systemen an Bedeutung.

So sollten EDR-Systeme (Endpoint Detection and Response Systeme) fast immer in kritischen Systemen verwendet werden. Diese sind Sicherheitstools, die kontinuierlich Daten von Endpunkten (z.B. Computer, Servern oder mobilen Geräten) sammeln und analysieren. Sie verwenden fortschrittliche Techniken, die auch unter Verwendung künstlicher Intelligenz und maschinellem Lernen, Muster identifizieren und Anomalien erkennen, die auf einen Sicherheitsvorfall hinweisen könnten[20].

Insbesondere sind EDR-Lösungen dafür konzipiert, auch Zero-Day-Exploits zu erkennen. Auch wenn der genaue Angriffsvektor eines Zero-Day-Exploits vorab nicht bekannt ist, können EDR-Lösungen durch die Analyse des Verhaltens und der Aktivitäten auf den Endpunkten dennoch Hinweise auf solche Angriffe geben. Das hätte in diesem Fall zumindest dazu geführt, dass der Angriff deutlich schneller hätte, gefunden werden.

Der Angriff lenkt zudem Aufmerksamkeit auf die zunehmende Bedrohung durch staatlich unterstützte Cyberangriffe, insbesondere aus China und Russland.
Andere Staaten könnten aus mehreren Gründen an Fortinet interessiert sein: Zum einen sind die Kunden von Fortinet oftmals Unternehmen und Institutionen, die für die nationale Sicherheit und die Wirtschaft von großer Bedeutung sind, so sind einige Staats- und Regionalbanken unter den Kunden[5]. Der Zugang zu deren Netzwerken könnte wertvolle Informationen liefern oder Möglichkeiten zur Störung oder Manipulation ganzer Staaten, Regionen oder Industriezweige bieten. Diese Bedrohung kann man seit 2014 im andauernden Ukrainekonflikt beobachten[21,22]. Zusätzlich könnte die Kenntnis der Technologien und Schutzmaßnahmen von Fortinet dazu dienen, eigene Cyber-Sicherheitsfähigkeiten zu verbessern oder umgekehrt effektivere Angriffe auf Ziele zu ermöglichen, die Fortinet-Technologien verwenden.

[5]Fortinet. (2022). Fortinet Global Customers and Case Studies. [online] Available at: https://www.fortinet.com/customers [Accessed 8 Jun. 2023].
[20]ISPIN AG Zurich. (2022). *Warum EDR für Ihre Cybersicherheit unverzichtbar ist*. [online] Available at: https://www.ispin.ch/news-events/blog/warum-edr-fuer-ihre-cybersicherheit-unverzichtbar-ist/# [Accessed 14 Jun. 2023].
[21] Muth, M. (2022). *Ukraine und Russland: Nie gab es mehr Cyberkrieg*. [online] Süddeutsche.de. Available at: https://www.sueddeutsche.de/wirtschaft/mircosoft-ukraine-cybersicherheit-russland-hackerangriff-it-sicherheit-1.5687083 [Accessed 14 Jun. 2023].
[22] Autoren der Wikimedia-Projekte (2022). *Angriff auf ukrainische Regierungswebseiten*. [online] Wikipedia.org. Available at: https://de.wikipedia.org/wiki/Cyberkrieg_im_Bezug_zum_Russland-Ukraine-Krieg [Accessed 14 Jun. 2023].

Diese Ereignisse verdeutlichen, dass die Cyber-Sicherheitslandschaft zunehmend von staatlich unterstützten Akteuren geprägt wird, die im Gegensatz zu privaten Hackern schier unbegrenzte Monetäre und Zeitliche Mittel haben. So können Systeme gekauft und damit sehr genau untersucht werden. Das verdeutlicht die Notwendigkeit, sowohl die technischen als auch die politischen Aspekte der Cyber-Sicherheit ernst zu nehmen und die Verteidigungsstrategien und -technologien kontinuierlich zu aktualisieren und zu verbessern.

Quellenangabe:

[0]Gartner. (2022). *Gartner Identifies Three Factors Influencing Growth in Security Spending*. [online] Available at: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i [Accessed 12 Jun. 2023].
[1]Microsoft.com. (2022). *Nation state threats | Microsoft Security*. [online] Available at: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-nation-state-attacks [Accessed 14 Jun. 2023]
[2] Marczak, B. (2021). *FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild - The Citizen Lab*. [online] The Citizen Lab. Available at: https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/ [Accessed 19 May 2023].
[3] Cloudflare. (2017). *Was war der WannaCry-Ransomware-Angriff?* [online] Available at: https://www.cloudflare.com/de-de/learning/security/ransomware/wannacry-ransomware/ [Accessed 19 May 2023].
[4] Autoren der Wikimedia-Projekte (2016). *Geschäftsbetrieb*. [online] Wikipedia.org. Available at: https://de.wikipedia.org/wiki/Fortinet#J%C3%BCngste_Entwicklung [Accessed 19 May 2023].
[5]Fortinet. (2022). Fortinet Global Customers and Case Studies. [online] Available at: https://www.fortinet.com/customers [Accessed 8 Jun. 2023].
[6] Q1 2023 Financial Results. (2023). Available at: https://investor.fortinet.com/static-files/f980ac27-60fc-467f-b154-899c2698311b [Accessed 19 May 2023].
[7] Fortinet, Inc. (2022). *Fortinet Reports Fourth Quarter and Full Year 2022 Financial Results | Fortinet, Inc.* [online] Available at: https://investor.fortinet.com/news-releases/news-release-details/fortinet-reports-fourth-quarter-and-full-year-2022-financial [Accessed 19 May 2023].
[8] Fortinet. (2022). *Next Generation Firewall (NGFW) – Top-Produkte anzeigen*. [online] Available at: https://www.fortinet.com/de/products/next-generation-firewall [Accessed 19 May 2023].
[9] Fortinet. (2022). *Erstklassiges Netzwerkverwaltungs-Softwaresystem & Operations-Tool | FortiManager*. [online] Available at: https://www.fortinet.com/de/products/management/fortimanager [Accessed 19 May 2023].
[10] Fortinet. (2022). *Netzwerkanalyse für große und komplexe Netzwerke | FortiAnalyzer*. [online] Available at: https://www.fortinet.com/de/products/management/fortianalyzer [Accessed 19 May 2023].
[11] Nist.gov. (2022). *NVD - CVE-2022-41328*. [online] Available at: https://nvd.nist.gov/vuln/detail/CVE-2022-41328#range-9013321 [Accessed 19 May 2023].
[12] Mandiant.com. (2023). Available at: https://www.mandiant.com/sites/default/files/inline-images/fig3-fortinet-malware-ecosystem.png [Accessed 20 May 2023].
[13] Django Project. (2023). *Django overview*. [online] Available at: https://www.djangoproject.com/start/overview/ [Accessed 20 May 2023].
[14]Mandiant. (2021). *Threat Intelligence & Cyber Security Company | Mandiant | EN*. [online] Available at: https://www.mandiant.de/company [Accessed 13 Jun. 2023].
[15] Mandiant.com. (2023). Available at: https://www.mandiant.com/sites/default/files/inline-images/fig4-fortinet-malware-ecosystem.png [Accessed 20 May 2023].
[16] Mandiant. (2022). *Fortinet Zero-Day and Custom Malware Used by Suspected Chinese Actor in Espionage Operation | Mandiant*. [online] Available at: https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem [Accessed 20 May 2023].
[17]Mandiant. (2022). *Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors | Mandiant*. [online] Available at: https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence [Accessed 20 May 2023].

[18]Mandiant. (2022). *Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475)* | *Mandiant*. [online] Available at: https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw [Accessed 13 Jun. 2023].
[19]Mandiant. (2022). *Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors* | *Mandiant*. [online] Available at: https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence [Accessed 13 Jun. 2023].
[20]ISPIN AG Zurich. (2022). *Warum EDR für Ihre Cybersicherheit unverzichtbar ist*. [online] Available at: https://www.ispin.ch/news-events/blog/warum-edr-fuer-ihre-cybersicherheit-unverzichtbar-ist/# [Accessed 14 Jun. 2023].
[21] Muth, M. (2022). *Ukraine und Russland: Nie gab es mehr Cyberkrieg*. [online] Süddeutsche.de. Available at: https://www.sueddeutsche.de/wirtschaft/mircosoft-ukraine-cybersicherheit-russland-hackerangriff-it-sicherheit-1.5687083 [Accessed 14 Jun. 2023].
[22] Autoren der Wikimedia-Projekte (2022). *Angriff auf ukrainische Regierungswebseiten*. [online] Wikipedia.org. Available at: https://de.wikipedia.org/wiki/Cyberkrieg_im_Bezug_zum_Russland-Ukraine-Krieg [Accessed 14 Jun. 2023].