Köln, 31. August 2023

Bundesamt für Verfassungsschutz

BfV Cyber-Brief Nr. 02/2023

Gruppierungen APT 15 und APT 31 nutzen Heimnetzwerkgeräte für staatlich gesteuerte Cyberangriffskampagnen

Gruppierungen APT 15 und APT 31 nutzen Heimnetzwerkgeräte für staatlich gesteuerte Cyberangriffskampagnen

Aktuelle Hinweise deuten auf die Bedrohung deutscher kleiner und mittelständischer Unternehmen (KMU) und Privathaushalte durch Cyberangriffe gegen Heimnetzwerk- bzw. Small Office/Home Office (SOHO)-Endgeräte hin. Diese Endgeräte, die für den Einsatz in Unternehmen geringerer Größe oder von Privatanwendern konzipiert sind, werden in wachsender Anzahl durch Cyberangreifer übernommen und in der Folge in Cyberangriffskampagnen durch die APT-Gruppierungen[1] APT 15 und APT 31 gegen staatliche und politische Stellen genutzt.

Zum Schutz dieser KMU und privater Haushalte und der über deren Endgeräte letztlich angegriffenen staatlichen und politischen Stellen enthält dieser Cyber-Brief nachfolgend eine detaillierte Erläuterung der Vorgehensweise von APT 15 und APT 31 sowie konkrete Handlungsempfehlungen.

Hintergrundinformationen

APT 15 ist eine seit Jahren sehr aktive Cyberspionagegruppierung, die in der Vergangenheit vor allem durch Angriffe auf diplomatische Ziele sowie auf Wirtschaftsunternehmen öffentlich bekannt wurde (vgl. Cyber-Brief Nr. 01/2020).[2]

Auch APT 31 ist eine sehr aktive Cyberspionagegruppierung, deren Cyberangriffe sich in den letzten Jahren vermehrt gegen Ziele in westlichen Ländern richteten. Hierunter fallen beispielsweise Ministerien, Behörden, politische Organisationen und Stiftungen (vgl. Cyber-Brief Nr. 01/2021).[3]

1 Advanced Persistent Threat (APT): Unter APT werden komplexe, zielgerichtete Bedrohungen verstanden, die sich gegen ein oder mehrere Opfer richten. Die konkreten Angriffe im Rahmen dieser Bedrohungen („threats“) werden von Angreifenden aufwändig vorbereitet, sich hoch entwickelt („advanced“) und dauern lange an („persistent“).

2 Der BfV Cyber-Brief 01/2020 von Juni 2020 bot auch technische Hinweise zur Detektion an und ist auf der BfV Website unter www.verfassungsschutz.de abrufbar.

3 Der BfV Cyber-Brief 01/2021 von Januar 2021 bot ebenfalls technische Hinweise zur Detektion an und ist auf der BfV Website unter www.verfassungsschutz.de abrufbar.

Sachverhalt

Dem Bundesamt für Verfassungsschutz (BfV) liegen Erkenntnisse über die Ausnutzung von kompromittierten Heimnetzwerk- bzw. SOHO-Endgeräten durch die Cybergruppierungen APT 15 und APT 31 vor. Die Endgeräte, die häufig von KMU sowie von Privathaushalten eingesetzt werden, werden durch die Angreifer für Cyberangriffskampagnen gegen staatliche und politische Stellen genutzt.

Vorgehensweise der Cyberangreifer

Schritt 1: Kompromittierung von Heimnetzwerk- bzw. SOHO-Endgeräten

Die Cyberangreifer kompromittieren Heimnetzwerk- bzw. SOHO-Endgeräte in großer Stückzahl. Anfällig für eine solche Kompromittierung sind insbesondere Geräte mit bekannten Schwachstellen, vor allem dann, wenn der Support durch den Hersteller eingestellt wurde (sogenannte „End-of-Life“-Geräte).

Als angegriffene Endgeräteklassen konnten bisher identifiziert werden:

- Heim- bzw. SOHO-Router,
- Netzwerkspeicher/-festplatten (sog. NAS-Systeme),
- SOHO-Firewall-Systeme,
- Smart Home- bzw. Home Automation-Systeme.

Alle zuvor genannten Endgeräteklassen sind – unabhängig vom Hersteller – im Laufe des Einsatzes von Schwachstellen betroffen. Umso wichtiger ist es, Sicherheitsupdates zeitnah einzuspielen und nicht mehr vom Hersteller unterstützte „End-of-Life“-Geräte auszutauschen. Das Spektrum geeigneter Ziele für Cyberangreifer, die sich auf solche Endgeräteklassen ausrichten, ist groß. Kompromittierbare Systeme lassen sich zudem mit geringer Fachkenntnis und speziellen Werkzeugen gezielt ermitteln.

Schritt 2: Einbindung in angreiferspezifische Verschleierungsnetzwerke

Verschleierungs- oder Anonymisierungsnetzwerke, im erweiterten Sinne auch als Virtual Private Networks (VPN) bezeichnet, dienen grundsätzlich der Sicherung einer Kommunikationsverbindung über das öffentliche Internet. Derartige Netzwerke existieren als Produkte kommerzieller VPN-Anbieter oder können als frei verfügbare Produkte genutzt werden, wie beispielsweise das TOR-Netzwerk. Als großer Vorteil gilt dabei im Allgemeinen das Verbergen der Ursprungs-IP-Adresse.

Die Cyberspionagegruppen APT 15 und APT 31 nutzen diesen Vorteil im Rahmen von Cyberangriffen zur Verschleierung ihrer Urheberschaft. Verschleierungsnetzwerke, die mutmaßlich speziell für die Cyberspionagegruppierungen unter Verwendung der in Schritt 1 kompromittierten Endgeräte erstellt wurden, kommen dabei zur Anwendung.

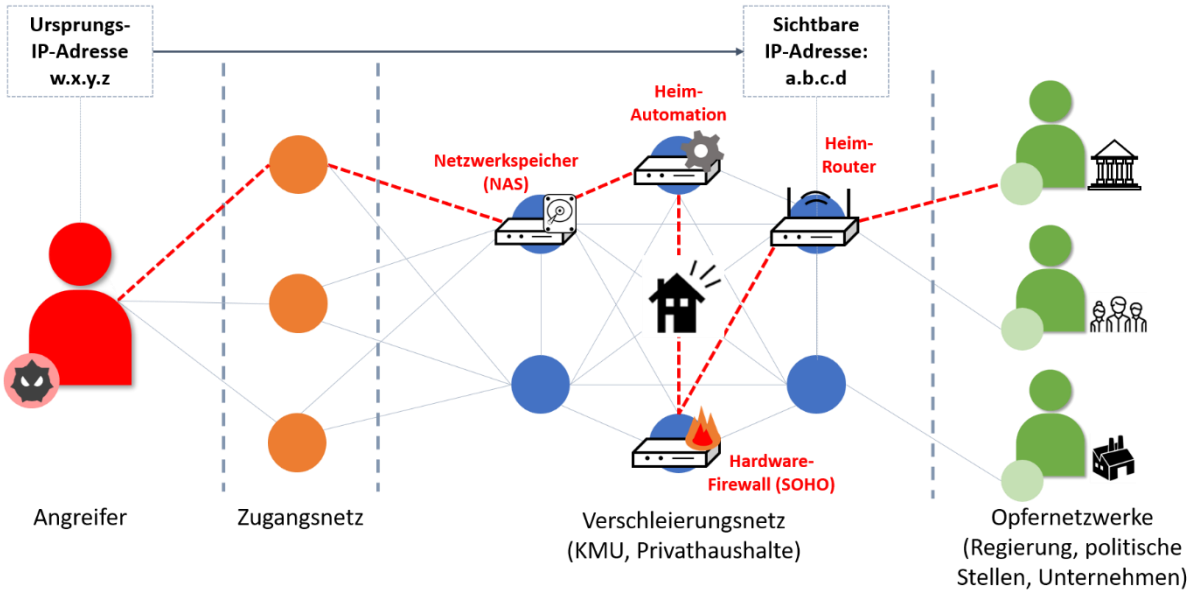

Abbildung: Schematische Darstellung eines Anonymisierungsnetzwerks

Wie in der Abbildung dargestellt, greift der Akteur (rot) zuerst auf einen Knoten in einem Zugangsnetz (orange) zu. Über das Zugangsnetz erfolgt dann der Zugriff auf das eigentliche Verschleierungsnetz (blau). Hier finden sich vor allem auch die zuvor genannten Heimnetzwerk- bzw. SOHO-Endgeräte. Über das Verschleierungsnetz greift der Akteur schließlich die eigentlichen Opfer (grün) an.

Die Kommunikationsverbindung (rot gestrichelt) wird über einen vom Angreifer vorbestimmten Weg zwischen den Netzwerkgeräten des Verschleierungsnetzwerks aufgebaut. Das Opfer erkennt dabei in der Regel nur die letzte Instanz der Verbindung – den Heim-Router mit dessen IP-Adresse als Angreifer. Die Ursprungs-IP-Adresse des Angreifers bleibt also verborgen. So erscheinen im Rahmen der Bearbeitung von staatlich gesteuerten Cyberangriffen, insbesondere der Gruppierungen APT 15 und APT 31, vermehrt IP-Adressen von KMU und Privathaushalten.

Schritt 3: Cyberangriff gegen die eigentlichen Ziele mithilfe des Verschleierungsnetzwerks

Mithilfe dieser kompromittierten Endgeräte und dem daraus entstehenden Angreifernetzwerk verüben die Gruppierungen Cyberangriffe zu Spionagezwecken vor allem gegen Regierungseinrichtungen und politische Organisationen. Auch Aktivitäten gegen Unternehmen zum Zwecke der Wirtschaftsspionage sind so möglich.

Die Detektion solcher Angriffsversuche ist für die angegriffenen Organisationen erschwert, da die eingehenden Verbindungen von privaten Internetanschlüssen in Deutschland wenig auffällig erscheinen. Alle drei Schritte verlaufen unbemerkt durch den Betreiber. Es treten in der Regel weder Verbindungsabbrüche noch anderweitige Auffälligkeiten auf.

Derzeit sind keine Fälle bekannt, in denen die Betreiber der Heimnetzwerk- bzw. SOHO-Endgeräten selbst Opfer eines Cyberangriffs wurden. Die Übernahme der Geräte in Schritt 1 erfolgte bisher ausschließlich zur Einbindung in die Verschleierungsnetzwerke, wie in Schritt 2 beschrieben.

Handlungsempfehlungen

KMU und Privathaushalte sollten handeln, um es Externen und damit auch Cyberspionagegruppierungen zu erschweren, in Firmen und Privathaushalten betriebene Endgeräte zu übernehmen und diese für Cyberangriffe gegen Regierungseinrichtungen und politische Organisationen einzusetzen.

Aus Sicht des BfV sind drei Schritte vorrangig:

Schritt 1: Risiken vermindern

- **Geräte kennen**

  Verschaffen Sie sich einen Überblick über die von Ihnen in Ihrem Netzwerk betriebenen Geräte wie Router, Netzwerk-Drucker und Netzwerkspeicher. Denken Sie dabei auch an Internet der Dinge- oder Smart Home-Geräte, wie beispielsweise Steuerungen für Rollläden, Licht, Heizungen oder Solaranlagen.

  Tragen Sie die Zugangsdaten für Management-Oberflächen aller entsprechenden Geräte zusammen. Achten Sie bei den Zugangsdaten auf eine sichere Verwahrung.

- **Zustand ermitteln**

  Ermitteln Sie den Zustand der betriebenen Geräte in Ihrem Netzwerk. Ist der Router noch auf der Höhe der Zeit? Hierbei sollten derzeitige Versionsstände der Geräte erfasst werden und im Hinblick auf Aktualisierungen geprüft werden.

  Viele Hersteller bieten ein automatisiertes Update-Verfahren über die Benutzeroberfläche ihrer Geräte an. Aufschluss hierüber gibt oftmals das Benutzerhandbuch. Sollten Sie die Funktion für automatisierte Updates aktiviert haben, prüfen Sie, ob die jeweiligen Geräte durch den Hersteller noch mit Updates versorgt werden.

  Seriöse Hersteller bieten meist einen transparenten Umgang mit Geräten, für die keine aktualisierten Programmversionen mehr zur Verfügung stehen („End-of-Life“-Geräte). Hierfür stellen sie auf Ihren Internetseiten entsprechende

Listen mit Gerätetypen oder andere Abfragemöglichkeiten bereit. Informieren Sie sich bei älteren Geräten, ob diese möglicherweise keine aktualisierten Programmversionen mehr erhalten.

Ersetzen Sie gegebenenfalls veraltete Geräte.

Schritt 2: Systeme härten

- **Aktualisierungen vornehmen**

  Spielen Sie bei nicht mehr aktueller Software auf Ihren Geräten bereitstehende (Sicherheits-)Updates zeitnah ein. Aktualisierungen vorzunehmen sollte für Sie zu den regelmäßigen Wartungsaufgaben für Ihre Geräte gehören. Machen Sie sich daher einen Plan und setzen Sie sich Erinnerungen.

- **Geräte im Netzwerk warten und pflegen**

  Aktualisieren Sie nicht nur einmal, sondern halten Sie Ihre Geräte beständig aktuell: Achten Sie auf entsprechende Hersteller-Informationen über bereitstehende neue Programmversionen/Updates oder Software zur Behebung von Programmfehlern, sogenannte Patches. Beachten Sie auch aktuelle Informationen und Hinweise zu Schwachstellen und Cyberangriffskampagnen. Nutzen Sie dabei auch das öffentliche Informationsangebot, beispielsweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI).[4]

- **Netzwerke sichern**

  In Ihre IT-Netze eingebundene Geräte wie die von Ihnen zugelassenen Zugriffsrechte für Externe öffnen Angreifern Tür und Tor. Prüfen Sie, ob ein Fernzugriff von außen/von unterwegs auf Ihre Heimnetzwerk- bzw. Smart Home-Endgeräte wirklich erforderlich ist. Entfernen Sie eventuell zuvor gesetzte Freigaben in den Firewall-Einstellungen an Ihrem Router, sobald diese nicht mehr benötigt werden. Wägen Sie auch ab, ob beispielsweise ein Webserver aus dem Büro- oder

4 Vgl. https://bsi.bund.de; Stichwort: „Verbraucherinnen und Verbraucher“.

Heimnetz betrieben werden muss oder ein qualifizierter Anbieter (ein sogenannter Hoster) diese Aufgabe übernehmen kann.

- **Cyberangreifer aussperren**

  Gestalten Sie die bei Ihnen im Einsatz befindlichen Betriebssysteme sowie Software- und Cloud-Anwendungen so, dass Sie nicht benötigte Zugänge schließen und nicht benötigte Funktionen abschalten oder ggf. deinstallieren. Mit einer solchen Härtung schützen Sie sich besser gegen Cyberangriffe aller Art.

  Prüfen Sie zudem, ob vom Hersteller vorgegebene Standardeinstellungen, insbesondere Sicherheitseinstellungen, für Ihren Einsatz sinnvoll geändert werden können.

Schritt 3: (Neue) Angriffsflächen ausschließen

- **IT-Sicherheit bei Ihren Kaufentscheidungen mitbedenken**

  Prüfen Sie bei Ihren Kaufentscheidungen, ob und wie lange Geräte, die Sie erwerben wollen, einen Support des Herstellers erhalten.

  Prüfen Sie bei Produkten mit Cloud-Anteilen wie z.B. Sicherheitskameras mit Cloudspeicher, wo und wie lange Daten gespeichert werden und wer darauf zugreifen kann. Wägen Sie ab, ob Sie dem Cloud-Anbieter Ihre Daten anvertrauen wollen.

- **Sichere Passwörter**

  Ändern Sie im Rahmen der vom Hersteller gegebenen Möglichkeiten gesetzte Standardpasswörter für Ihre Geräte.

  Setzen Sie insbesondere bei Zugängen von außen komplexe Passwörter ein. Nutzen Sie dabei die Hinweise des BSI zur Erstellung sicherer Passwörter.[5]

5 Vgl. https://bsi.bund.de; „BSI-Basisschutz: Sichere Passwörter“.

Aktivieren Sie, wenn möglich, eine Multi-Faktor-Authentisierung, so schaffen Sie mehr Sicherheit für Ihre vernetzten Geräte und Online-Konten.

Weitere Informationen

Weitere Informationen über staatlich gesteuerte Cyberangriffe erhalten Sie auf der Website des BfV.[6] Hier finden Sie, neben dem Verfassungsschutzbericht des Bundes, weitere Cyber-Briefe, die Sicherheitshinweise für Wirtschaft sowie Politik und Verwaltung, die Informationsblätter Wirtschaftsschutz sowie das Faltblatt „Cyberangriffe: Gefahren erkennen – Risiken minimieren“. Diese Materialien des BfV bieten zusätzliche Handlungsempfehlungen zum Schutz vor Cyberangriffen.

6 Vgl. www .verfassungsschutz.de.

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Abteilung 4
Merianstraße 100
50765 Köln
poststelle@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 228/99 792-0
Fax: +49 (0) 228/99 792-2600

Bildnachweis
© maxsim | fotolia.com

Stand
August 2023