Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

Zyxel Firewalls zur Verbreitung von Ransomware missbraucht

CSW-Nr. 2024-290907-1032, Version 1.0, 22.11.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

In den vergangenen Tagen kam es wiederholt zu Berichten über Unternehmensnetzwerke, die mit der Ransomware Helldown infiziert wurden. Die Täter nutzten Helldown einerseits zur Verschlüsselung der dortigen Datenträger, andererseits drohten sie den Opfern aber auch mit der Veröffentlichung zuvor ausgeleiteter Informationen (Double Extortion).
Erste Vorfälle dieser Art wurden im August 2024 beobachtet, eine weitere größere Welle an Angriffen erfolgte im Oktober [SEK24].

Bei der Analyse fanden IT-Sicherheitsforschende heraus, dass zur Durchführung der Angriffe in den meisten Fällen vermutlich eine Schwachstelle in Zyxel Firewalls ausgenutzt wurde. Bislang ist jedoch unklar, um welche Schwachstelle es sich im Detail handelt und ob diese überhaupt öffentlich bekannt ist. [SEK24][TRS24]

Am 21. November veröffentlichte Zyxel ein Security Advisory und bestätigte den Bericht von Sekoia über Helldown Ransomware-Angriffe und gab an, dass die dabei ausgenutze Sicherheitslücke in der neuesten Firmware-Version 5.39, die am 3. September veröffentlicht wurde, nicht reproduzierbar sei und daher Kunden mit neuster Firmware und getauschten Zugangsdaten nicht länger bedroht seien. [ZYX24a] [ZYX24a]

Verwundbar sind sowohl die Firewall-Serien:

- Zyxel USG Flex als auch
- Zyxel ATP.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Trotz des damit seit September verfügbaren Patches berichteten einige Institutionen auch zu späteren Zeitpunkten von Helldown-Infektionen, obwohl der bereitgestellte Patch kurzfristig installiert worden war [ZYX24b].

Weitere Untersuchungen förderten nun zutage, dass die alleinige Aktualisierung der betroffenen Geräte nicht ausreichend war, um eine Kompromittierung nachhaltig zu verhindern. Stattdessen können die Angreifenden angelegte Accounts nutzen, um in die Netzwerke einzudringen. Weitere Details zum Ablauf der Angriffe können den Blogs von Truesec [TRSE24] und Sekoia [SEK24] entnommen werden. IT-Sicherheitsverantwortliche müssen daher zusätzliche Maßnahmen anstoßen.

Hierzu zählt insbesondere die Änderung sämtlicher Passwörter, die bei der Nutzung der Zyxel-Firewalls relevant sind. Darüber hinaus sollte überprüft werden, ob neue, unbekannte Accounts in jüngerer Vergangenheit angelegt wurden. Empfehlungen hierzu können auch den Veröffentlichungen des Herstellers [ZYX24a], [ZYX24b] entnommen werden.

Bewertung

Firewalls stellen aufgrund ihrer zentralen Bedeutung für Netzwerke in Organisationen attraktive Ziele für Cyber-Angriffe dar. Mithilfe einer Kompromittierung können dort verarbeitete Daten sabotiert bzw. ausspioniert werden oder weiterführende Attacken - z.B. Lateral Movement - gestartet werden.

Der vorliegende Sachverhalt unterstreicht gleichzeitig, dass die alleinige Nutzung von Benutzername/Passwort-Kombinationen keinen hinreichenden Sicherheitsmechanismus zur Authentifizierung von Usern im Internet darstellen. Insbesondere für Administrative-Konten sollte unbedingt 2-Faktor Authentifizierung eingesetzt werden. Gleichzeitig sollten Auffälligkeiten beim Betrieb per Monitoring protokolliert werden.

Die Ransomware Helldown und die dazugehörige Leak-Seite wurde erstmals am 13. August 2024 beobachtet. Nach Kenntnislage des BSI wurden auf der Leak-Seite bis 21.11.2024 32 mutmaßlich Betroffene durch die Angreifer genannt, hiervon wurden 5 mutmaßlich Betroffene aus Deutschland beobachtet.

Dem BSI sind keine Entschlüsselungstools für diese Ransomware bekannt. Nach vorläufiger Kenntnislage basiert Helldown auf dem veröffentlichten Builder der bekannten Ransomware LockBit, welcher seit September 2022 von verschiedenen Angreifern als Grundlage für neue Ransomware herangezogen wird. Das von Strafverfolgern im Rahmen der Operation Cronos veröffentlichte Entschlüsselungstool für LockBit funktioniert für Helldown nicht, da es auf sichergestelltem Schlüsselmaterial basiert.

Mögliche Auswirkungen auf Kritische Infrastrukturen inkl. Verwaltung

Der geschilderte Vorfall kann in ähnlicher Art auch Kritische Infrastrukturen treffen und die dargestellten Konsequenzen haben.

Fragen an IT-Sicherheitsverantwortliche

IT-Sicherheitsverantwortliche sollten insbesondere Folgendes prüfen:

Präventiv:

- Sind ALLE Passwörter sämtlicher Accounts auf den betriebenen Zyxel-Firewalls und im Active Directory geändert worden?
- Kann sichergestellt werden, dass die neu gesetzten Passwörter nicht bereits in der jüngeren Vergangenheit verwendet wurden?
- Wurden über externe Authentifizierungsserver (z.B. Radius) verwaltete Kennwörter von Administrator-Konten gewechselt?
- Sind Pre-Shared-Keys der VPNs ausgetauscht worden?
- Ist auf allen Zyxel-Firewalls ein aktueller Patch-Stand installiert?
- Können Zugriffe auf die Firewall mithilfe der Umsetzung zusätzlicher IT-Sicherheitsmaßnahmen [ZYX24c] [ZYX24d] – z.B. Multi-Faktor-Authentifizierung (MFA) – weiter abgesichert werden?
- Ist der Zugriff auf die Web-Oberfläche über WAN deaktiviert? Falls nicht möglich, sollte mindestens der Zugriff nur von spezifizierten IP-Adressen erlaubt werden.

Reaktiv:

- Kann ausgeschlossen werden, dass auf den betriebenen Zyxel-Firewalls nicht autorisierte Administratoren- bzw. Benutzeraccounts eingerichtet wurden? Bislang im Kontext von Angriffen beobachtete Konten hatten u.a. die Bezeichnungen "SUPPORT87", "SUPPOR817" oder "VPN", aber auch andere. Ungewöhnliche Uhrzeiten können ein zusätzlicher Indikator sein.
- Welche der unter [TRS24] und [SEK24] angebotenen Indicators of Compromise können in der eigenen Institution genutzt werden?
- Wurden Logs auf verdächtige VPN-Verbindungen – insbesondere aus dem Ausland – geprüft?
- Ist sichergestellt, dass keine unautorisierten Anpassungen von Firewall-Regeln stattgefunden haben?
- Wurden Firewall-Regeln, die den Zugriff von WAN, SSL-VPN-Zonen oder Any erlauben, entfernt?
- Ist die Abmeldung unbekannter, aktiver Accounts erzwungen worden?
- Sind unbekannte, inaktive Accounts auf den Firewalls gelöscht worden?
- Werden regelmäßig Recherchen zu verfügbaren Helldown-Entschlüsselungstools durchgeführt?
- Sind die BSI-Empfehlung zur Bedrohung "Ransomware" in der Institution bekannt? [BSI24]

IT-Sicherheitsverantwortliche können unten genannte Quellen nutzen, um Hilfestellungen zur Absicherung von Zyxel Firewalls zu erhalten.

Links

[TRS24] Helldown Ransomware Group – A New Emerging Ransomware Threat:
https://www.truesec.com/hub/blog/helldown-ransomware-group

[SEK24] Helldown Ransomware: an overview of this emerging threat:
https://blog.sekoia.io/helldown-ransomware-an-overview-of-this-emerging-threat/

[ZYX24a] Zyxel security advisory: protecting against recent firewall threats:
https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-protecting-against-recent-firewall-threats-11-21-2024

[ZYX24b] Zyxel Community - Ransomware Helldown
https://community.zyxel.com/en/discussion/26764/ransomware-helldown

[ZYX24c] Zyxel USG FLEX and ATP series – Upgrading your device and ALL credentials to avoid hackers' attacks
https://support.zyxel.eu/hc/en-us/articles/21878875707410-Zyxel-USG-FLEX-and-ATP-series-Upgrading-your-device-and-ALL-credentials-to-avoid-hackers-attacks

[ZYX24d] Zyxel Community - Best Practices to Secure a Distributed Network Infrastructure
https://community.zyxel.com/en/discussion/10920/best-practices-to-secure-a-distributed-network-infrastructure/p1?new=1

[BSI24] Ransomware – Fakten und Abwehrstrategien:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?
   Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4. Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.