Eurofit Informationstechnologie GmbH
Schillerstraße 2, A-4020 Linz

Informationen über den Angriff ZyXEL Firewalls

Version 1.03 (06.07.2021)

Frage 1: Worum geht es überhaupt?

Wir haben am Montag, den 14.06.2021 gegen 09:30 Uhr von einem Kunden die Information erhalten, dass eine IPsec Verbindung nicht ordnungsgemäß funktioniert. Die erste schnelle Analyse hat mehr Fragezeichen als Antworten ergeben, weil die VPN Verbindung aktiv, aber ein Datenaustausch darüber nicht möglich war. Tiefgründigere Analysen haben in weiterer Folge ergeben, dass das VPN Netzwerk-Routing abgehend nicht korrekt funktioniert und entsprechende Datenpakete nicht in den VPN Tunnel gesendet werden. Die Ursache dafür war eine zusätzliche Policy-Route Einstellung, die aber offensichtlich nicht von uns durchgeführt wurde. Weitere Prüfungen der Konfiguration haben ergeben, dass auf der Firewall ein zusätzlicher Benutzer mit administrativen Berechtigungen angelegt wurde. An diesem Punkt war klar, dass die Konfiguration der Firewall von einem unberechtigten Dritten böswillig verändert wurde.

Frage 2: Wann und wie lange hat dieser Zustand angehalten?

Es war keine langfristige Protokollierung auf Firewall oder ein externes Logging aktiviert. Diese Frage können wir daher nicht gezielt beantworten. Unsere letzte Interaktion mit der betroffenen Firewall war am 19.04.2021 um 09:35 Uhr. Hier wurde ein Firmware Update mit wichtigen Sicherheitsupdates installiert und auch die Konfiguration der Firewall von uns gesichert. Diese Konfiguration weist noch keine Manipulationen auf. Der Sicherheitsvorfall hat daher zwischen 19.04.2021 09:35 Uhr und 14.06.2021 09:00 stattgefunden. Die Konfigurationsänderung, die zu einem Ausfall der VPN Verbindung geführt hatte, wurde zwischen 11.06.2021 und 14.06.2021 durchgeführt. Ob zwischen 19.04.2021 und 11.06.2021 unberechtigte Zugriffe auf die Firewall oder das Netzwerk dahinter erfolgten, können wir nicht nachvollziehen.

Frage 3: Wurden bei dem betroffenen System Daten gestohlen?

Die Transferstatistiken der betroffenen Internet Verbindung zwischen 11.06.2021 und 14.06.2021 wiesen keine Auffälligkeiten auf. Ein größerer Datenabzug ist daher sehr unwahrscheinlich. Nach einem detaillierten Review der manipulierten Konfiguration stellten wir fest, dass die zum Zeitpunkt des Abzugs der manipulierten Konfiguration am 14.06.2021 11:19:09 durchgeführten Änderungen funktional nicht lauffähig waren, um einen Zugriff des angelegten SSLVPN Benutzers zu ermöglichen. Es ist aber nicht auszuschließen, dass zwischenzeitlich auch eine funktionell lauffähige Konfiguration bestanden hatte, die unbefugte Zugriffe in das Netzwerk erlaubt hätte.

Tel: +43 (732) 652732-0
Fax: +43 (732) 652732-11
Email: office@eurofit.at
Web: www.eurofit.at
Firmenbuch: FN79730
UID: ATU41393504
DVR: 1031503
Gerichtsstand: Linz
Zahlungen an: Oberösterreichische Landesbank AG
BIC: OBLAAT2L
IBAN: AT92 5400 0000 0025 2080

Frage 4: Können wir ausschließen, dass Daten gestohlen wurden?

Die klare Antwort lautet: **nein**.

Frage 5: Welche Gegenmaßnahmen wurden auf dem betroffenen System unternommen?

Wir haben die manipulierte Konfiguration der Firewall für weitere Analysen gesichert und die als bekannt gute Konfiguration vom 19.04.2021 wiederhergestellt.
Zur Wahrung der Sicherheit wurden umgehend folgende weiteren Maßnahmen gesetzt:

- Ändern des Admin Kennworts der Firewall. Das Kennwort war 14 Zeichen lang, komplex und zufällig generiert.
- Update der Firewall Firmware auf die letzte Version 4.63.0 (vom 31.05.2021). Inzwischen ist jedoch bekannt, dass auch die aktuelle Firmware von dem Sicherheitsproblem betroffen ist.
- Ändern der IPsec Pre-Shared Keys
- Aktivieren des GEO-IP Filters, um externe https Zugriffe (für Konfiguration und SSL VPN) auf die Firewall auf Österreich als Herkunftsland zu beschränken.
- Kontaktieren des Hersteller-Supports, da die Vermutung nahe lag, dass das Gerät durch eine Sicherheitslücke übernommen wurde. ZyXEL Deutschland hat uns am 23.06.2021 gegen 18 Uhr bestätigt, dass mehrere derartige Fälle bekannt sind und damit die Integrität der Firewalls nicht mehr gewährleistet werden kann. Mit Stand 24.06.2021 15:00 ist noch keine Lösung verfügbar, die das zu Grunde liegende Problem nachhaltig korrigiert.
- Implementierung von Multi-Faktor Authentifizierung über Google Authenticator für die administrative Anmeldung an der Firewall über Web und SSH.

Frage 6: Welche Maßnahmen sind im Moment angebracht?

Wir überprüfen seit 24.06.2021 13:30 Uhr proaktiv sämtliche Firewalls aller aktiven Kunden auf eine etwaige Kompromittierung. Sollten wir eine weitere betroffene Firewall identifizieren, werden wir die in Punkt 5 angeführten Maßnahmen umsetzen und mit Ihnen direkt Kontakt aufnehmen, um die Gefahrensituation im Detail zu besprechen.
Im Zuge der ersten Überprüfungsmaßnehmen wurde kein weiteres von uns betreutes Gerät identifiziert, das erfolgreich angegriffen und manipuliert wurde.

Frage 7: Welche Maßnahmen sind in weiterer Folge angebracht?

- Am 27. Juni 2021 wurde von ZyXEL Firmware 4.64 bzw. 5.01 veröffentlicht, die hilft, die Angriffsfläche zu minimieren. Unter anderem wurde die Verwendung des GEO-IP Filters ohne Content Filter ermöglicht. Das zu Grunde liegende Problem konnte zu diesem Zeitpunkt jedoch noch nicht identifiziert werden.
- Am 06. Juli 2021 wurde von ZyXEL Firmware 4.65 und 5.02 veröffentlicht, die das zu Grunde liegende Sicherheitsproblem nun tatsächlich schließt. Der Sicherheitslücke wurde am 02. Juli 2021 die ID CVE-2021-35029 vergeben, siehe https://cve.report/CVE-2021-35029. Dieses Firmware Update ist auf allen Geräten so rasch wie möglich zu installieren. Da diese neuen Versionen unter Umständen ein

Tel: +43 (732) 652732-0
Fax: +43 (732) 652732-11
Email: office@eurofit.at
Web: www.eurofit.at
Firmenbuch: FN79730
UID: ATU41393504
DVR: 1031503
Gerichtsstand: Linz
Zahlungen an: Oberösterreichische Landesbank AG
BIC: OBLAAT2L
IBAN: AT92 5400 0000 0025 2080

funktionelles Problem mit externen SIP Telefonie Anbindungen haben, müssen wir in entsprechenden Umgebungen unter Umständen noch auf eine 5.02 basierte ITS WK Version warten, die auch diese Korrektur beinhaltet.

- Ändern des Web Konfigurations-Ports von 443 auf zum Beispiel 8443. Zur Wahrung der Business Continuity kann der SSL VPN Port auf 443 verbleiben. Die entsprechende Funktionalität wurde für die USG Serie mit Firmware 4.64 Ende Juni 2021 nachgeliefert.
- Nicht mehr unterstützte Firewalls der ersten USG Generation (2006 – 2014) sind zwingend auszutauschen.

~~**Frage 8: Können wir uns nachhaltig schon vor Verfügbarkeit eines Updates vor dieser Sicherheitslücke schützen?**~~

~~Ja, wenn Sie auf die SSLVPN Funktionalität verzichten. Sollte die SSLVPN Funktion bei Ihnen nicht verwendet werden, werden wir die Möglichkeit für einen Extern-Zugriff auf das Webinterface Ihrer Firewall gemäß Punkt 6 im Zuge der ersten Durchsicht abstellen, falls dieser überhaupt aktiv ist. Üblicherweise exponieren wir das Webinterface standardmäßig **nicht** ins Internet, sofern es nicht technisch erforderlich ist.~~

Frage 9: Werden alle Firewalls das erforderliche Update erhalten?

Nein. Firewalls der ersten ZLD Generation (bis Firmware 3.30, ZyWall USG 20, USG20W, USG 50, USG 100, USG 200, USG 300 und USG 1100) haben das letzte Firmware-Update im Dezember 2016 erhalten und werden von ZyXEL nicht mehr gepflegt. Wir werden mit den betroffenen Kunden in Kontakt treten und empfehlen den Umstieg auf ein neues Gerät – wenn das durch das erforderliche Update dann auch wieder sicher ist.

Frage 10: Fallen uns Kosten für die Überprüfung und das erforderliche Update an?

Ja, wir verrechnen unsere Dienstleistung gemäß unserer Wartungsvereinbarung. Da es in diesem Fall maßgeblich um rasches Handeln geht, holen wir von Ihnen kein Einverständnis ein, um die erforderlichen Punkte 6 und 7 umzusetzen.

Frage 11: Sind vom Hersteller ZyXEL direkt auch Informationen über den Angriff und den aktuellen Status verfügbar?

Ja. Bitte lesen sie folgenden Support Artikel: https://support.zyxel.eu/hc/de/articles/4402786248466

Frage 12: Was wurde im Detail an der Firewallkonfiguration geändert (nur für „Nerds“ oder technisch interessierte Personen von Belang)?

```
username manage encrypted-password
$5$szIztqXA$ZZ1I6XiC$5/i7OoycXcerWlw0iFk0aYk46wy06VrPApWMqSJYxS9PdgK2m8wAFBmIULGJrpSbvLsCl9v
oWnCdBI+UckdwI8bEOOE04AbJXHknEvxSB1pKcZy/BHcUzSuR5iGIOsGYmfW90274i9IluBbRZlEQL2KncMD9pEbL+NJ
u1YEdELVFXc0Un0K6IqxQ9I6sXsXhEgU3igMUFZRVpfS5gmemQS4ZM0daHosoOYVZ2IYY9SoUEzsW82uu200ZHjnXdzh
```


Tel: +43 (732) 652732-0
Fax: +43 (732) 652732-11
Email: office@eurofit.at
Web: www.eurofit.at

Firmenbuch: FN79730
UID: ATU41393504
DVR: 1031503
Gerichtsstand: Linz

Zahlungen an: Oberösterreichische Landesbank AG
BIC: OBLAAT2L
IBAN: AT92 5400 0000 0025 2080

```
W/mLfKH7nUQnDh7Pwog6tjk+MPYOK07vWaQt7FQIk+gVVFSa3Dk/UMocX5i4QVkEsEocLxHnBEIQ4RLXiP+hqH4SIzeF
FamlmjlixQj7n4aU$ user-type admin

username manage description Local User

username manage logon-time-setting default

username zyxel_sllvpn encrypted-password
$5$keQxpdnu$FLbvpqNL$Pex3VknZR0OYiDqRyeH43dUbgTSxIKMx+RC0ppipnzhgk5hwUOifMUGtwOvn8oaHm8GFjRk
gnzZX2ncSayj6k59m5aWFo2Y6uDo+TTxraoBL/pOITtqm+jXjN1d6svjo/qoXF02Apa6gEOGNSr09Joy62+BZSsFLDfv
+p+LZW0NZf3dEIvQr+vNyJJJ0NzlTQQ+S1dnUmuWd1zo0VYKrq0rzNxPTWUUCxTep410WOggYD0MKPPaV2LrpzO1kR/e
2Z/gCm52gvkNg3iapcZY/mRMdh8T/ws8qh4TKZIg07APdx8tcGkJa9Ujx/FkTXWAY1sLVnFQ3ng1i2m0pvMy0DoRqAs+
kj6CBtP2x36doLec$ user-type user

username zyxel_sllvpn description Local User

username zyxel_sllvpn logon-time-setting default
```

Diese Befehle legen zwei zusätzliche Benutzer an, wobei der Benutzer „manage“ administrative Berechtigungen erhalten hat.

```
sslvpn policy sslvpn_index

 description sslvpn_index Create

 network-extension activate

 user zyxel_sllvpn

 network-extension network LAN1_SUBNET

 network-extension network NET_EFIT_Linz_WAN_Liwest

 network-extension network NET_EFIT_Linz_WAN_Lagis

 network-extension network NET_xxx_LAN

 network-extension network NET_xxxx_LAN

 network-extension network NET_xxxxx_WLAN

 network-extension network NET_EFIT_Linz_LAN

 network-extension network NET_EFIT_Steyr_LAN

 network-extension netbios-broadcast

 network-extension ip-pool LAN1_SUBNET
```

Diese Befehle aktivieren eine zusätzliche SSLVPN Richtlinie, die dem oben angelegten neuen Benutzer „zyxel_sllvpn“ die Möglichkeit haben, die hier angeführten Netze über SSLVPN grundsätzlich erreichen zu können.

```
zone SSL_VPN

 sslvpn xxx_SSLVPN

 sslvpn sslvpn_index
```

Dieser Befehl fügt die oben angelegte SSLVPN Verbindung in die Sicherheitszone SSL_VPN ein.

Tel: +43 (732) 652732-0
Fax: +43 (732) 652732-11
Email: office@eurofit.at
Web: www.eurofit.at
Firmenbuch: FN79730
UID: ATU41393504
DVR: 1031503
Gerichtsstand: Linz
Zahlungen an: Oberösterreichische Landesbank AG
BIC: OBLAAT2L
IBAN: AT92 5400 0000 0025 2080

```
policy 1
 description loseang
 source LAN1_SUBNET
 dscp any
 next-hop auto
 snat outgoing-interface
```

Diese Befehle sorgen dafür, dass Datenpakete aus dem Kunden Netzwerk automatisch an die am besten passende Verbindung weitergeleitet werden und eine Netzwerkadressübersetzung der ausgehenden Schnittstelle erhalten. Im konkreten Fall bewirkt diese Regel aber einen Bruch der Infrastruktur und ein Nicht-Funktionieren sämtlicher IPsec VPN Verbindungen.

Weiters haben wir festgestellt, dass die Firewall-Regeln selbst offenbar nicht angepasst wurden. Aufgrund dieser Tatsache und unserer Best-Practice Regeln war ein Zugriff aus der SSL_VPN Zone in andere VPNs gar nicht möglich, auch nicht der Zugriff auf das Kunden-Netzwerk, weil dafür eine Gruppenmitgliedschaft des neuen Benutzers „zyxel_sllvpn“ erforderlich gewesen wäre, diese aber gefehlt hat.

Solange also zwischenzeitlich keine „bessere“ Konfiguration bestanden hat, war kein Zugriff auf das interne Netzwerk möglich – dies aber nur deshalb, weil der Angriff vermutlich automatisiert ausgeführt wurde und keine Rücksicht auf eine spezifische Konfiguration der Firewall genommen wurde. Die Firewall ist aber kompromittiert und erlaubt es dem Angreifer, jederzeit die Konfiguration so anzupassen, dass auch Zugriff in das interne Netzwerk auch tatsächlich möglich ist.

Die Netzwerknamen unseres initial betroffenen Kunden wurden zur Wahrung des Datenschutzes in „xxx“ geändert.

Wir werden dieses Dokument aktualisieren, wenn neuen Informationen verfügbar sind.

Tel: +43 (732) 652732-0
Fax: +43 (732) 652732-11
Email: office@eurofit.at
Web: www.eurofit.at
Firmenbuch: FN79730
UID: ATU41393504
DVR: 1031503
Gerichtsstand: Linz
Zahlungen an: Oberösterreichische Landesbank AG
BIC: OBLAAT2L
IBAN: AT92 5400 0000 0025 2080