SX-GATE

Software Update
Release Note

Version: 7.0-5-2

Inhaltsverzeichnis

1 Wichtige Informationen

Die in dieser Release Note enthaltenen Informationen beruhen auf sorgfältiger Recherche. Dennoch läßt es sich nicht ausschließen, dass eine Information im Einzelfall unzutreffend ist. Wir bitten daher um Ihr Verständnis, wenn wir keine Gewähr für die Richtigkeit der Informationen übernehmen und jede Haftung ausschließen. Sollten Sie feststellen, dass eine Information unzutreffend ist, bitten wir um Ihre Rückmeldung.

Richten Sie Ihre Rückmeldung bitte an die folgende E-Mail Adresse: support@xnetsolutions.de

1.1 Technische Unterstützung

Um technische Unterstützung bei der Durchführung des Software-Updates zu erhalten, können Sie unseren technischen Support via Telefon oder E-Mail erreichen. Wenn Sie den technischen Support kontaktieren, halten Sie bitte folgende Informationen bereit:

- momentan installierte SX-GATE Software-Version
- Geräte-ID
- SX-GATE Support-IP-Adresse

Diese Informationen können Sie über die Startseite auslesen.

So erreichen Sie den technischen Support:

Rufnummer:	+49 (0) 7032-95596-21
E-Mail:	support@xnetsolutions.de

1.2 Vorbereitung

Das Update der Systemsoftware erfolgt mit einer Update-Datei, um alle notwendigen Komponenten und Subsysteme intelligent zu aktualisieren. Die aktuelle Update-Datei enthält dabei alle vorherigen Updates seit dem letzten Update auf eine Hauptversion. Die Updates sind immer in der Reihenfolge der Versionsnummerierung zu installieren.

Hinweis:

Die Folge eines unterbrochenen Update-Vorgangs könnte sein, dass Ihr SX-GATE nicht mehrt bootet. Schalten Sie das SX-GATE deshalb nicht aus oder führen einen manuellen Neustart durch, während das Update durchgeführt wird. Sollte ein Neustart notwendig sein, wird dies durch das Update automatisch durchgeführt.

1.3 Installation

Bitte beachten Sie, dass Ihr SX-GATE die erforderlichen Voraussetzungen erfüllen muss, bevor Sie dieses Software-Update Installieren.

- **Arbeitsspeicher mindestens 2048 MB (2 GB) - optimal mindestens 4096 MB (4 GB)**

Sie können die aktuelle Speicherbestückung in der Konfigurationsoberfläche **auf der Startseite** einsehen. Für alle Fragen bzgl. des Software-Updates wenden Sie sich bitte an den technischen Support.

Gehen Sie folgendermaßen vor, um ein Software-Update durchzuführen:

Hinweis:

Erstellen Sie bitte vor dem durchführen des Software-Updates ein System-Backup, ein Benutzer-Backup und ein E-Mail-Backup.

Für das Durchführen eines Software-Updates haben Sie die folgenden Möglichkeiten:

- **Automatisches Software-Update über die SX-GATE Konfigurationsoberfläche**

Führen Sie über das Menü **»System → Update«** ein interaktives Software-Update durch. Wählen Sie dazu die Option **»interaktiv (empfohlen)«** und folgen Sie den Anweisungen auf dem Bildschirm. Wählen Sie im folgenden die Schaltfläche **»Weiter«**, um das Update automatisch zu installieren. Über das Fortschreiten des Software-Updates und einen bei Bedarf erforderlichen Reboot des SX-GATE werden Sie im interaktiven Update-Log informiert.

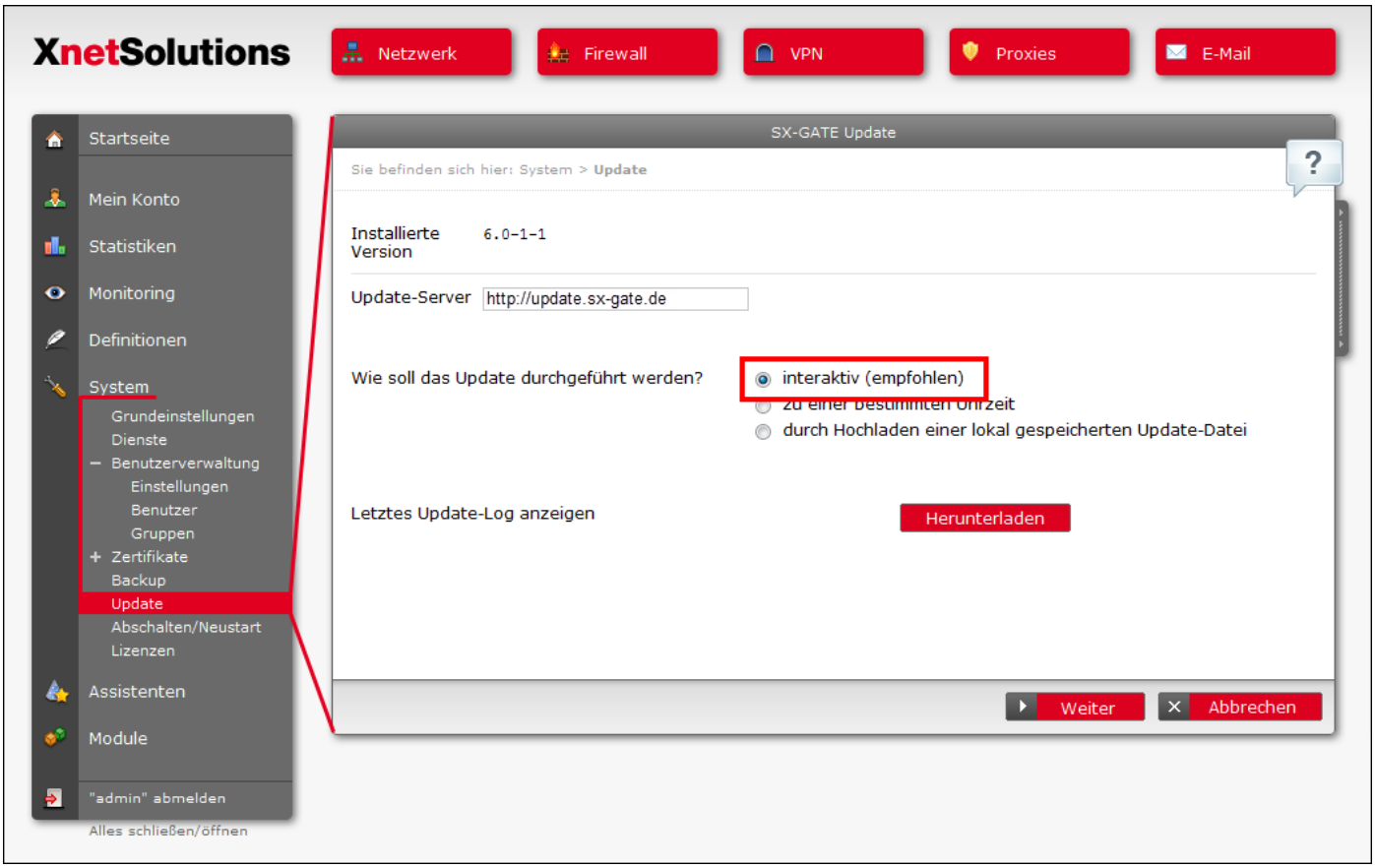

Abbildung 1 - Menü »System → Update«

- **Manuelles Software-Update**

Bevor Sie das Software-Update durchführen können ist es erforderlich, dass Sie das benötigte Software-Update Version 7.0-5-2 von der SX-GATE Update-Webseite herunterladen.

Die Update-Webseite erreichen Sie unter http://www.xnetsolutions.de → Menü **»Support -> Software Updates«**.

Führen Sie über das Menü **»System → Update«** ein manuelles Software- Update durch. Wählen Sie dazu die Option »durch Hochladen einer lokal gespeicherten Update-Datei« und folgenden Sie den Anweisungen auf dem Bildschirm.

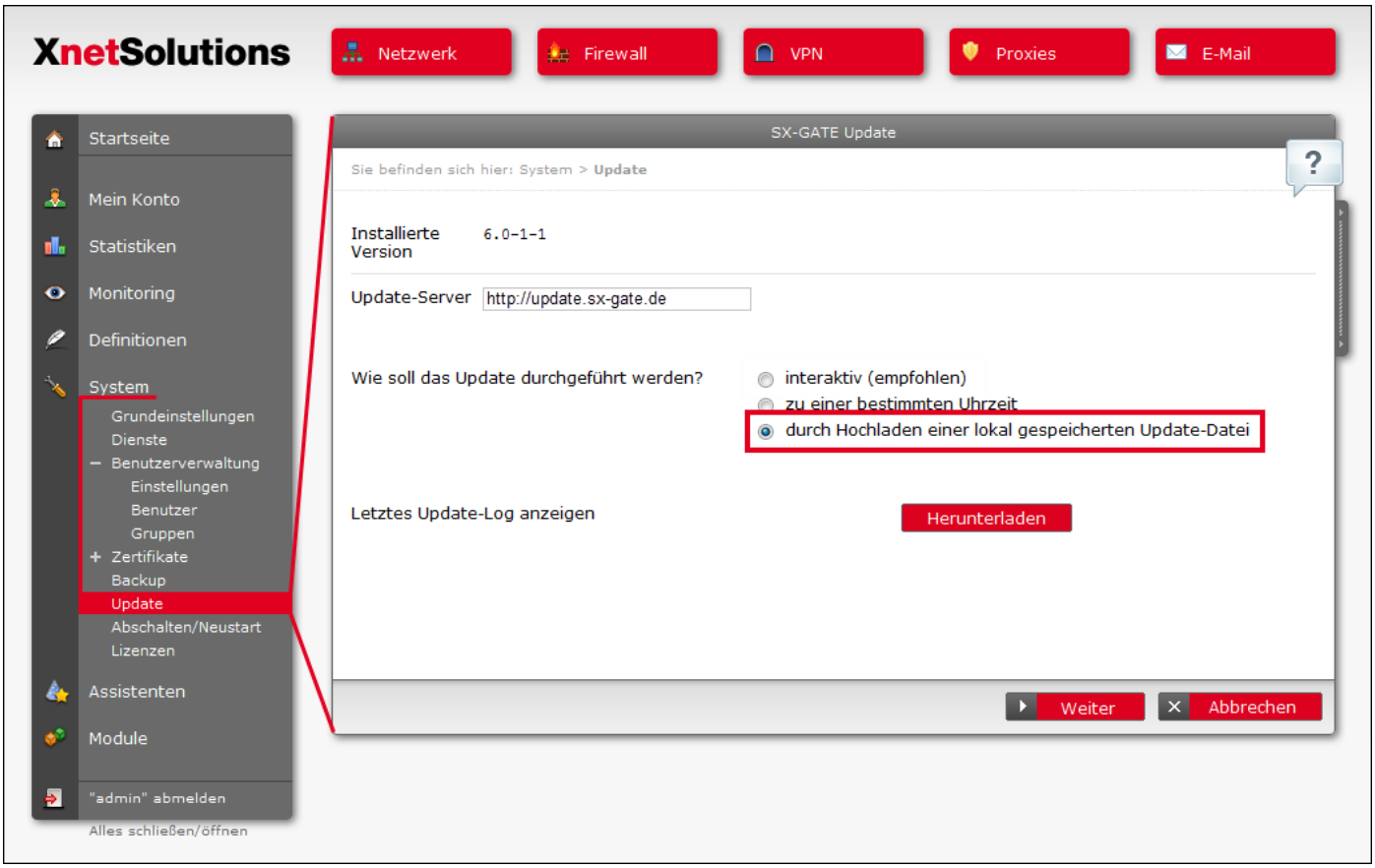

Abbildung 2 - Menü »System → Update«

Wichtig:

Der Update-Vorgang kann, je nach Größe des Updates und Leistungsfähigkeit des SX-GATE, einige Zeit in Anspruch nehmen.

2 Änderungen in dieser Software-Version

Neustart erforderlich

Nach dem Update führt das System automatisch einen oder mehrere Neustarts durch. Bitte führen Sie keinen manuellen Reboot durch! Das System kann dadurch funktionsunfähig werden.

2.1 Bugfix

2.1.1 Avira Antivirus

Aufgrund einer falsch konfigurierten Update-Prozedur konnte sich der Scanner nach dem Signatur-Update vom 14.01.2020 gegen 16:00 Uhr nicht mehr mit den Servern für Online-Abfragen verbinden.

2.2 Update

2.2.1 Let's Encrypt-Zertifikate

Der Client zum Abruf von Let's Encrypt-Zertifikaten nutzt ab jetzt das Protokoll ACMEv2.

3 Änderungen in vorherigen Versionen

3.1 Version 7.0-5-1

3.1.1 Sicherheitskritisch

3.1.1.1 Aktualisierung POP3-/IMAP4-Server

Das Update behebt ein kritisches Sicherheitsproblem. Einem Angreifer war es damit ohne Authentifizierung möglich, geschützte Informationen auszulesen oder sogar eigenen Programmcode auszuführen.

3.2 Version 7.0-5-0

3.2.1 Bugfix

3.2.1.1 Aktualisierung des Linux-Kernels

Mit speziellen TCP-Paketen konnte ein Angreifer einen Systemabsturz verursachen oder hohe Systemlast erzeugen.

3.2.1.2 Keine Verbindung zu Mail-Servern möglich, die bei der Verschlüssung ausschließlich ECDSA unterstützen

3.2.2 Sicherheitskritisch

3.2.2.1 Abruf von E-Mails aus der Quarantäne

Im Quarantäne-Modus "E-Mails zurückhalten" mit aktiviertem Benutzerzugriff wurde den Empfängern fälschlicherweise auch für E-Mails mit gefährlichem Inhalt ein Link für das Zustellen der E-Mail gesendet.
Die Quarantäne-Modi "Anhang entfernen" und "E-Mail abweisen" sind nicht betroffen. Systeme mit deaktiviertem Benutzerzugriff sind ebenfalls nicht betroffen.

3.2.3 Update

3.2.3.1 Virenscanner-Engines von Avira, F-Secure und Kaspersky

3.2.3.2 Zahlreiche Software-Pakete

3.2.3.3 IDS/IPS-Signaturen für Systeme ohne Pflegevertrag

3.2.3.4 URL-Filter Datenbank

3.3 Version 7.0-4-9

3.3.1 Sicherheitskritisch

3.3.1.1 Aktualisierung des Linux-Kernels und der CPU-Microcodes

Das Update enthält Gegenmaßnahmen für die unter dem Sammelbegriff "Microarchitectural Data Sampling" (MDS) zusammengefassten Sicherheitslücken in Intel-CPUs. Um die Sicherheitslücke ausnutzen zu können, muss ein Angreifer eigenen Code auf dem System zur Ausführung bringen.

Bei virtuellen Systemen besteht die Gefahr, dass Gast-Systeme auf Daten des Hosts oder anderer Gäste zugreifen können. Stellen Sie daher sicher, dass auf dem Host geeignete Maßnahmen gegen MDS ergriffen wurden.

Vollständig geschützt ist das System nur, wenn Hyperthreading deaktiviert wird, was sich jedoch stark auf die Leistungsfähigkeit auswirkt. Wir halten diese Maßnahme nicht für notwendig, da normalerweise nur Code aus vertrauenswürdigen Quellen auf dem System ausgeführt wird. Es steht Ihnen jedoch frei, Hyperthreading selbständig im BIOS zu deaktivieren.

3.4 Version 7.0-4-8

3.4.1 Sicherheitskritisch

3.4.1.1 Aktualisierung des Linux-Kernels

Der neue Kernel enthält einige weniger kritische sicherheitsrelevante Bugfixes.

3.4.2 Bugfix

3.4.2.1 Fehlfunktion des F-Secure Antivirus

Am Nachmittag des 10.04.2019 kam es aufgrund fehlender Zugriffsrechte auf eine neue Bibliotheksdatei zu einer Fehlfunktion des F-Secure Antivirus-Scanners. Die Datei wurde im Zuge der Signatur-Updates installiert.

3.4.2.2 Benutzersynchronisation aus dem ActiveDirectory

In Version 7.0-4.7 schlägt die Benutzersynchronisation fehl.

3.4.2.3 Aktualisierung des IPsec-Servers

Die neue Version behebt Probleme beim IKEv2 Re-keying.

3.5 Version 7.0-4-7

3.5.1 Bugfix

3.5.1.1 F-Secure Antivirus

Seit 05.02.2019 meldet der F-Secure-Virenscanner fälschlicherweise "Scanner-Test fehlgeschlagen" bzw. "F-Secure Linux Security funktioniert nicht". Der Scanner wird mittels EICAR-Testfile auf Funktion geprüft. Diese schlägt fehl, da sich das Format der Ausgabe geändert hat.

Die Funktion des Virenscanners war zu keiner Zeit beeinträchtigt.

3.6 Version 7.0-4-6

3.6.1 Bugfix

3.6.1.1 E-Mail Dateianhangs-Filter und kennwortgeschützte RAR-Archive

Der Dateianhangs-Filter bleibt bei der Verarbeitung von E-Mails mit kennwortgeschützten RAR-Archiven hängen, wenn die Option zum prüfen von ZIP- und RAR-Archiven aktiviert ist. Nach Ablauf eines Timeouts wird die Mail mit einem temporären Fehler abgewiesen.

Wichtiger Hinweis:
Betroffen von dem Problem ist die seit Anfang November 2018 aktive Welle von Verschlüsselungstrojanern mit Bewerbungs-Emails. Werden Mails per SMTP empfangen, hat der Fehler den Empfang der Viren verhindert. Werden Mails jedoch von einem POP-Server abgerufen, liegen die Viren noch im Postfach und werden nach der Installation des Updates abgerufen. Wir empfehlen vor dem Update die Mitarbeiter über diese Gefahr zu informieren oder, soweit noch nicht geschehen, RAR-Dateien zumindest vorübergehend im MIME-Filter zu sperren.

3.6.2 Sicherheitskritisch

3.6.2.1 SSH-Server

Das Update beseitigt zwei weniger kritische Sicherheitsproblem im SSH-Server. Ab sofort werden keine Algorithmen mit CBC Blockverschlüsselung mehr akzeptiert. Ferner war es in älteren Versionen möglich, anhand des Timing-Verhaltens zu ermitteln, ob es ein bestimmtes Benutzerkonto im System gibt.

3.7 Version 7.0-4-5

3.7.1 Sicherheitskritisch

3.7.1.1 Aktualisierung des Linux-Kernels

Dieser Kernel enthält kleinere Verbesserungen und Fehlerbehebungen, bezüglich des kürzlich eingeführten Schutzes für die Intel-CPU Sicherheitslücke "L1 Terminal Fault" (L1TF).

Hinweis:
Bei virtuellen Systemen besteht die Gefahr, dass Gast-Systeme auf Daten des Hosts oder anderer Gäste zugreifen können. Stellen Sie daher sicher, dass auf dem Host geeignete Maßnahmen gegen L1TF ergriffen wurden.

3.7.2 Bugfix

3.7.2.1 Reverse-Proxy

Seit der Aktualisierung des Reverse Proxy in 7.0-4.3 ist es möglich, dass Teile des Prozesse in einer Endlosschleife weiterlaufen können, wenn Clients unerwartet die Verbindung abbrechen. Dies kann zu einer außergewöhnlich hohen Belastung führen und das gesamte System beeinflussen.

Hinweis:
Sollte das System schon unter einer erhöhten Last stehen, ist es sinnvoll den Reverse Proxy Dienst oder eventuell das gesamte System vor dem Update neu zu starten, da der Updatevorgang sonst unnötig ausgebremst wird.

3.8 Version 7.0-4-4

3.8.1 Sicherheitskritisch

3.8.1.1 Aktualisierung des Linux-Kernels

Der Kernel schützt gegen die neuerliche Intel-CPU Sicherheitslücke "L1 Terminal Fault" (L1TF).

Hinweis:
Bei virtuellen Systemen besteht die Gefahr, dass Gast-Systeme auf Daten des Hosts oder anderer Gäste zugreifen können. Stellen Sie daher sicher, dass auf dem Host geeignete Maßnahmen gegen L1TF ergriffen wurden.

3.8.1.2 Samba Windows-Client Bibliothek

Mit überlangen Dateinamen in Verzeichnis-Listings konnte ein Puffer-Überlauf in der Windows-Client Bibliothek ausgelöst werden.

3.9 Version 7.0-4-3

3.9.1 Sicherheitskritisch

3.9.1.1 Aktualisierung des Linux-Kernels

Das Update enthält Microcode Updates für die Intel-CPUs von Geräten, die ab Januar 2010 (19"-Geräte) bzw. Januar 2012 (Standgeräte) ausgeliefert wurden. Die Microcodes schützen vor den unter dem Sammelbegriff "Spectre-NG" bekanntgewordenen "neuen" Prozessorfehlern "Spectre V3a" und "Spectre V4". Verbessert wird zudem der Schutz gegen den "alten" Fehler "Spectre V2".

Hinweis:
Schutzmaßnahmen gegen "Spectre V1", "Spectre V2" und "Meltdown" (V3) sind bereits seit Version 7.0-3.3 bzw. 7.0-3.4 enthalten.

3.9.2 Bugfix

3.9.2.1 Intrusion Prevention und Firewall

Durch die Intrusion Prevention wurden sporadisch TCP-Reset-Pakete verworfen. Dies zog ein erhöhtes Aufkommen von ungültigen Paketen nach sich. Zusammen mit einer in Version 7.0-4.0 erfolgten Änderung im Bewertungssystem der dynamischen Firewall konnte dies dazu führen, dass IP-Adressen fälschlicherweise gesperrt wurden.

Im Rahmen des Bugfixes wurde die Protokollierung ungültiger Pakete überarbeitet. In unkritischen Fällen findet eine Protokollierung nun erst bei starker Häufung statt.

3.9.2.2 Web-Proxy Content-Filter

Mit bestimmten Clients konnte es insbesondere bei sehr großen Downloads vorkommen, dass die Verbindung vom Proxy getrennt wurde, noch bevor die letzten Daten an den Client übermittelt wurden.

3.9.3 Update

3.9.3.1 Reverse-Proxy

Neben verbesserten Schutzfunktionen unterstützt die neue Version WebSocket-Verbindungen.

3.10 Version 7.0-4-2

3.10.1 Sicherheitskritisch

3.10.1.1 Aktualisierung des Linux-Kernels

In Intel Prozessoren wurde eine Sicherheitslücke bekannt, über die ein Angreifer, der eigenen Code zur Ausführung bringen kann, Zugriff auf vertrauliche Daten innerhalb der Floating-Point-Unit (FPU) erhalten kann. Die FPU wird unter anderem für hardwarebeschleunigte Crypto-Operationen genutzt. Mit dem Update wird vom dafür anfälligen Lazy-FPU-Modus auf den Eager-FPU-Modus umgestellt.

3.10.1.2 Empfehlung zur Sperrung zusätzlicher Dateinamenserweiterungen

Im "MIME-Filter" des Mail-Servers und in der URL-Filter Liste "standard" des Web-Proxies empfehlen wir zusätzlich "iqy" und "slk" zu sperren. Beide Endungen werden aktuell von Schädlingen genutzt. Sie finden die komplette Liste der von uns zur Sperrung empfohlenen Dateiendungen in der Online-Hilfe zu den jeweiligen Konfigurationstabellen.

3.10.2 Bugfix

3.10.2.1 Nach einem Wechsel der Zeitzone wurde stets die alte Zeitzone angezeigt

3.10.3 Update

3.10.3.1 Neue Version des Greylist-Filters mit datenschutzkonformer Datenbank

3.11 Version 7.0-4-1

3.11.1 Bugfix

3.11.1.1 Interaktives Update

Auf Systemen, die vor dem 15. Juni 2018, 10:00 Uhr auf Version 7.0-4.0 aktualisiert wurden, wird während des nächsten Update-Vorgangs kein Protokoll angezeigt, sofern der "interaktive" Update-Modus gewählt wurde. Es wird lediglich "Der Updatevorgang läuft" angezeigt. Mit der Meldung "Es wurde ein Update geplant für: Kein wartender Auto-Update-Job!" ist das Update des Systems abgeschlossen. Im Hintergrund wird dann die Administrationsoberfläche aktualisiert. In dieser Zeit kann es zu Problemen beim Zugriff auf die Oberfläche kommen.

Um den Fortschritt des Updates dennoch verfolgen zu können, klicken Sie bitte gleich nach dem Start des Updates erneut auf den Menüpunkt "System > Update". Über "Letztes Update-Log anzeigen" öffnet sich ein neues Fenster mit dem Protokoll. Nutzen Sie die "Aktualisieren"-Funktion des Browsers, um die Anzeige aufzufrischen.

3.11.1.2 IPsec Server-Verbindungen mit Preshared-Key

In Version 7.0-4.0 wurden eingehende IPsec-Verbindungen von Dritthersteller-Routern wie insbesondere der FritzBox fälschlicherweise abgewiesen, wenn zur Authentifizierung ein Preshared-Key verwendet wird, für die Gegenstelle eine feste IP konfiguriert ist und die Gegenstelle XAuth-Unterstützung signalisiert aber nicht verwendet.

3.11.1.3 URL-Filter Datenbank

Seit der Aktualisierung der kostenfreien URL-Filter Datenbank in 7.0-4.0 wurden einzelne Google URLs fälschlicherweise in der Kategorie "Pornographie" geführt.

3.11.1.4 Firewall-Konfiguration in Administrations-Oberfläche

Der Reiter "Transp. Proxy", der in der Firewall-Konfiguration von LAN- und RAS-Schnittstellen angezeigt werden sollte, war in Version 7.0-4.0 ausgeblendet. Die Funktion der Firewall wurde dadurch nicht beeinträchtigt.

3.12 Version 7.0-4-0

3.12.1 Neu

3.12.1.1 Speicherdauer für E-Mail-Quarantäne

Die vorgegebene Speicherdauer von E-Mails im Quarantäne-Verzeichnis wurde auf 7 Tage reduziert, kann aber nun über die Administrations-Oberfläche geändert werden. Bitte prüfen Sie, welche Speicherdauer hier im Sinne des Datenschutzes vertretbar ist.

3.12.1.2 Bridging

In dieser Versionsreihe nur auf Systemen mit Software Pflegevertrag verfügbar.

Ethernet-, VLAN- und WLAN-Schnittstellen können in einer Bridge zusammengeschaltet werden. Für Verbindungen innerhalb der Bridge und für Verbindungen aus der Bridge heraus erfolgt dabei die Firewall-Konfiguration individuell je Port. Somit ist auch der Betrieb als transparente Firewall zwischen zwei Netzwerk-Segmenten möglich (z.B. zwischen LAN und Router). Für Verbindungen in eine Bridge hinein ist die Firewall-Konfiguration lediglich je Bridge, nicht aber je Port möglich.

3.12.1.3 Radius-Client für WLAN-Verbindungen

Bei Hardware mit WLAN-Option lässt sich nun WPA2-EAP Authentifizierung konfigurieren.

3.12.2 Bugfix

3.12.2.1 IPsec XAuth- und L2TP-Clients über selben NAT-Router

Parallele IPsec-Verbindungen mit XAuth- und L2TP-Clients waren nicht möglich, wenn sich die Clients hinter dem selben NAT-Router befinden.

3.12.3 Update

3.12.3.1 URL-Filter

Die URL-Filter Software und die kostenfreie URL-Datenbank wurden aktualisiert.

3.12.3.2 IDS/IPS-Signaturen für Systeme ohne Pflegevertrag

3.12.3.3 Virenscanner-Engines von Avira, F-Secure und Kaspersky

3.12.4 Änderung

3.12.4.1 Logdateien und Statistiken

Die Aufbewahrungsdauer von Logdateien und die Inhalte der Statistiken wurden unter dem Aspekt des Datenschutzes überarbeitet.

Logdateien werden künftig nur noch maximal 7 Tage aufbewahrt. Dazu werden die Logdateien nun nicht mehr wöchentlich sondern täglich archiviert. Beim Einspielen des Updates werden ferner alle Logdateien der vergangenen Wochen gelöscht und nur die gerade aktive Logdatei der aktuellen Woche aufbewahrt. Sofern die externe Achivierung von Logdateien konfiguriert ist, wird während des Updates eine entsprechende Warnung bzgl. Datenschutz oder notwendiger Anpassungen angezeigt.

Die Firewall-Statistiken enthalten IP-Adressen zukünftig nur noch in anonymisierter Form (192.168.x.x). In den Statistiken zu Proxies, Web- und E-Mail-Server sind keine Auswertungen nach Client-IP, Benutzername oder E-Mail-Adresse mehr enthalten. Nach dem Einspielen des Updates bleibt bei allen Statistiken nur die Übersichtsseite über die letzten 12 Monate erhalten. Die Seiten mit den Monats-Statistiken werden gelöscht. Um Mitternacht wird dann die Monats-Statistik für den aktuellen Monat neu generiert.

3.12.5 Sicherheitskritisch

3.12.5.1 Aktualisierung des Linux-Kernels

Der neue Kernel verbessert den Schutz gegen den "Spectre"-Angriff und behebt kleinere Lücken mit denen das System zum Absturz gebracht werden kann.

3.12.5.2 RC4 bei SMTP-Verbindungen

Bei verschlüsselten SMTP-Verbindungen war noch die unsichere RC4-Verschlüsselung zugelassen. Diese wurde entfernt.

3.13 Version 7.0-3-5

3.13.1 Neue Funktionen

3.13.1.1 Bündelung von Netzwerkkarten

In dieser Versionsreihe nur auf Systemen mit Softwarewartung verfügbar.

Netzwerkkarten lassen sich nun Bündeln um eine redundante Verbindung mit Switches herzustellen oder den Durchsatz zu erhöhen.

3.13.1.2 URL-Filter Meldung beim Aufbrechen von SSL-Verbindungen

In dieser Versionsreihe nur auf Systemen mit Softwarewartung verfügbar.

Beim Aufbrechen von SSL-Verbindungen im Web-Proxy wurde eine neue Option hinzugefügt, die die Darstellung von Sperr-Meldungen des URL-Filters betrifft. Ist eine Domain komplett gesperrt, hat der Proxy bisher schon den Verbindungsaufbau abgewiesen. Im Browser wurde daher nur eine allgemeine Fehlermeldung angezeigt, wonach der Proxy die Verbindung verweigert. Mit der neuen Option kann alternativ dazu der Verbindungsaufbau zunächst erlaubt werden, so dass dann die konkrete Sperr-Meldung des URL-Filters im Browser angezeigt wird.

3.14 Version 7.0-3-4

3.14.1 Sicherheitskritisch

3.14.1.1 Aktualisierung des Linux-Kernels

Gegen die spekulative Ausfühung von Befehlen in modernen Prozessoren wurde ein Angriff bekannt, über den Speicherbereiche ausgelesen werden können, auf die ein Prozess eigentlich keinen Zugriff hat, sofern ein Angreifer eigenen Schadcode zur Ausführung bringen kann (der sog. Angriff "Spectre"). Der aktualisierte Kernel versucht beide Varianten dieses Angriffs mit Hilfe von Speicherbarrieren und der sog. Retpoline-Technik zu erschweren.

3.14.2 Neue Funktionen

3.14.2.1 IP-Objekt vom Type "Host"

Das neue IP-Objekt steht für jeweils eine IPv4-, IPv6- und MAC-Adresse. Alle drei Werte sind dabei optional. In den meisten Fällen werden lediglich die IP-Adressen verwendet. Bei Einstellungen, die auch die MAC-Adresse verwenden, ist dies in der Dokumentation angegeben.

3.14.2.2 Firewall-Regeln auf Basis von MAC-Adressen

Um eine Firewall-Regel für eine MAC-Adresse zu spezifizieren, können Sie als Quelle ein IP-Objekt vom Typ "Host" auswählen. Ist in dem Objekt ausschließlich eine MAC-Adresse hinterlegt, gilt die Firewall-Regel für alle Pakete, die von dieser MAC empfangen wurden. Wurde zusätzlich mindestens eine der IPs im Objekt eingetragen, muss sowohl die MAC-Adresse als auch die IP übereinstimmen. Um eine Firewall-Regel für mehrere "Hosts" zu konfigurieren, können die "Host"-Objekte in Gruppen-Objekten zusammengefasst werden.

3.14.2.3 Benutzerspezifische Meldung nach Anmeldung an Administrations-Oberfläche

In dieser Versionsreihe nur auf Systemen mit Softwarewartung verfügbar.

In der Benutzerverwaltung kann bei Benutzern mit Zugriff auf die Administrations-Oberfläche (Gruppe "system-admin") eine Meldung hinterlegt werden, die jedesmal angezeigt wird, nachdem sich der Benutzer angemeldet hat.

3.14.3 Update

3.14.3.1 Diverse Softwarekomponenten

3.15 Version 7.0-3-3

3.15.1 Sicherheitskritisch

3.15.1.1 Aktualisierung des Linux-Kernels

In Intel-Prozessoren wurde eine Sicherheitslücke bekannt, die es ermöglicht, geschützte Speicherbereich auszulesen, sofern ein Angreifer eigenen Schadcode zur Ausführung bringen kann (der sog. Angriff "Meltdown"). Der aktualisierte Kernel verhindert diesen Angriff mit Hilfe der Technik Kernel-Page-Table-Isolation (KPTI).

Ferner wurde im Linux-Kernel eine Sicherheitslücke beseitigt, die es lokalen Benutzern erlaubt, erweiterte Zugriffsrechte zu erlangen.

3.15.2 Bugfix

3.15.2.1 Web-Proxy URL-Filter

Regeln die bedingungslosen Vollzugriff erlaubten funktionierten seit 7.0-3.1 nicht mehr.

3.15.2.2 UMTS-/LTE-USB-Sticks

Seit 7.0-3.1 wurden die Mobilfunk-USB-Sticks nach Stromverlust nicht mehr in den Modem-Modus umgeschaltet.

3.15.3 Neu Funktionen

3.15.3.1 Kommentarfeld für Anmeldung an Administrations-Oberfläche

Auf der Anmeldemaske der Administrations-Oberfläche kann ein Kommentar angegeben werden, der im Log aufgezeichnet wird. Hier lässt sich z.B. der Grund der Anmeldung, eine Ticket-Nummer oder der Name des Bearbeiters angeben.

3.16 Version 7.0-3-2

3.16.1 Bugfix

3.16.1.1 Zugriff auf google.de beim Aufbrechen von SSL-Verbindungen

Nach der kürzlich erfolgten Erneuerung der Zertifikate von google.de war kein Zugriff mehr möglich, da der OCSP-Status des Intermediate-CA-Zertifikats vom Proxy nicht akzeptiert wurde.

3.16.1.2 Abstürze des IPsec-Servers

Der IPsec-Server aus 7.0-3.1 konnte zum Absturz gebracht werden, wenn eine Gegenstelle eine Verschlüsselung ohne Integritätssicherung vorschlug. Normalerweise werden diese Algorithmen ignoriert.

3.16.1.3 DOS-Prüfung bei "Traceroute und ICMP-Ping beantwortet Firewall"

In Version 7.0-3.1 wurde bei aktivierter Firewall-Option "Traceroute und ICMP-Ping beantwortet Firewall" eine DOS-Prüfung mit niedrigem Grenzwert durchgeführt. Betroffen waren weitergeleitete Verbindungen mit Ausnahme von TCP. Insbesondere VoIP-Verbindungen wurden dadurch gestört.

3.17 Version 7.0-3-1

3.17.1 Sicherheitskritisch

3.17.1.1 Laden neuer IDS/IPS-Signaturen und -Konfiguration

Nach dem Rotieren von Logdateien konnte es vorkommen, dass die Intrusion-Prevention und die Intrusion-Detection Signale zum Laden neuer Signaturen oder geänderter Konfguration ignoriert.

3.17.2 Neu

3.17.2.1 Lesezugriff auf Administrationsoberfläche

In dieser Versionsreihe nur auf Systemen mit Softwarewartung verfügbar.

Der "admin" kann jetzt Benutzern der Gruppe "system-admin" Leseberechtigung auf die wichtigsten Konfigurationsmenüs erteilen. So lässt sich beispielsweise ein Auditor-Zugang realisieren. Bisher konnte der "admin" anderen Benutzern nur den Vollzugriff auf einzelne Menüs erlauben.

3.17.2.2 URL-Filter Benutzergruppen aus Active-Directory

In dieser Versionsreihe nur auf Systemen mit Softwarewartung verfügbar.

Der URL-Filter kann Benutzergruppen nun direkt aus dem Active-Directory auslesen. Voraussetzung ist ein Computer-Konto in der Windows-Domäne, wie es auch für die NTLM-Authentifizierung des Proxies erforderlich ist.

3.17.2.3 Zusätzliche Kategorien beim kostenpflichtigen URL-Filter

Neu sind folgende Kategorien: Malware, dynamische Adressen, "Datensammeln von Microsoft", Religion und Suchmaschinen.

3.17.3 Update

3.17.3.1 IPv6-Unterstützung in URL-Filter Regeln

Mit der neuen Version des URL-Filters können IPv6-Adressen nun auch als Client-IP in den Regeln konfiguriert werden. Bisher wurden IPv6-Adressen nur in Ziel-URLs unterstützt.

3.17.3.2 Diverse Softwarekomponenten

Unter anderem werden der Linux-Kernel, der DNS-Server, Samba und die OpenSSL Kryptobibliothek aktualisiert.

3.17.3.3 Aktualisierung der statischen SPAM-Filter Regeln

3.17.4 Änderung

3.17.4.1 Auswahllisten in der Administrations-Oberfläche

Bei der Auswahl von z.B. Protokollen oder IP-Objekten können die Auswahllisten sehr lang werden. Bei mehr als 20 Einträgen werden Sie jetzt durch eine Filterfunktion und durch Gruppierung der Einträge unterstützt.

3.17.5 Bugfix

3.17.5.1 Installation von automatisch verlängerten Zertifikaten über ACME

Über ACME verwaltete Zertifikate z.B. von Let's Encrypt werden zwar automatisch verlängert, in 7.0-3.0 schlägt dann jedoch die Installation in den Server-Diensten fehl. Die Installation wird nachgeholt, wenn die komplette Systemkonfiguration neu geschrieben wird. Dies ist regelmäßig nach Updates der Fall, auf einem Cluster-Master sogar nach jeder Synchronisierung der Konfiguration.

3.17.5.2 Update des IPsec Server

Die neue Version behebt Speicherlöcher sowie einen Absturz beim eingehenden Verbindungsaufbau mit bestimmten Verschlüsselungsparametern.

Bestehen zwischen zwei IPsec-Servern mehrere Tunnel und mindestens einer davon befindet sich hinter einem NAT-Router, konnte es nach Verbindungsabbrüchen wie z.B. einer täglichen DSL-Neueinwahl vorkommen, dass nicht mehr alle Tunnel neu aufgebaut werden. Auch dieses Problem ist nun behoben.

3.17.5.3 Verbesserter IPsec-Durchsatz

Der Durchsatz von breitbandingen IPsec-Verbindungen konnte durch Änderungen am L2TP-Server und in der Intrusion-Prevention gesteigert werden.

3.17.5.4 Berechtigungsprobleme in 7.0-3.0

Aufgrund geänderter Berechtigungen kam es in 7.0-3.0 zu Problemen bei folgenden Funktionen: Web-Server-Verzeichnisse und -Statistik, FTP-Zugriff auf E-Mail-Quarantäne und Archivierung von Logdateien.

3.18 Version 7.0-3-0

3.18.1 Bugfix

3.18.1.1 E-Mail Dateianhangs-Quarantäne

Das erste Problem betrifft ausschließlich Installationen, bei denen problematische Anhänge aus E-Mails entfernt werden und zusätzlich der Administrator den Empfängern Zugriff auf den Quarantänebereich gestattet. Wurde bei einer E-Mail mehr als ein Anhang unter Quarantäne gestellt, konnten die Empfänger nur den ersten Anhang herunterladen.

In einzelnen Installationen, bei denen E-Mails mit problematischen Anhängen komplett zurückgehalten werden, wurden die Benachrichtigungs-Mails an die Empfänger und ggf. den Administrator nicht gesendet.

3.18.1.2 IP-Objekte vom Typ "Geolokation"

Bisher wurden nur max. 15 Ländercodes pro IP-Objekt unterstützt.

3.18.2 Neu

3.18.2.1 Zertifikate von Let's Encrypt

In dieser Versionsreihe nur auf Systemen mit Software Pflegevertrag verfügbar.

Ab sofort können Zertifikate automatisiert über das ACME-Protokoll aktualisiert werden, was die Nutzung von kostenlosen Let's Encrypt-Zertifikaten ermöglicht. Eine entsprechende Alternative steht im Menü "Schlüsselbund" beim Ausstellen neuer Zertifikate zur Verfügung. Die Authentifizierung erfolgt dabei über das Verfahren "http-01". Sie müssen dazu den Reverse-Proxy auf Port 80 aus dem Internet erreichbar machen, virtuelle Hosts für die gewünschten Domains anlegen und darin jeweils das vordefinierte Backend "ACME HTTP-Authorisierung" aktivieren.

Eine Kurzanleitung finden Sie auf unserer Webseite im Menü "Support" > "SX-GATE" > "Anleitungen und Konfigurationsbeschreibungen".

3.18.2.2 Avira und Kaspersky Online-Abfrage

Um das Zeitfenster zwischen der Meldung eines neuen Virus an die Antivirenhersteller bis zum Download der neuen Signaturen besser zu überbrücken, bieten Avira und Kaspersky die Möglichkeit an, den Status verdächtiger Dateien online abzufragen. Dazu wird eine Prüfsumme über die Datei gebildet und an den Anbieter übermittelt.

In der Grundeinstellung ist diese Option aktiviert. Sie können sie im Menü "Module > Virenscanner" für jeden Scanner separat deaktivieren.

3.18.2.3 Avira Makro-Erkennung im Web-Proxy

In dieser Versionsreihe nur auf Systemen mit Software Pflegevertrag verfügbar.

In Kombination mit dem Avira Virenscanner lassen sich im Web-Proxy Content-Filter Office-Dokumente blockieren, wenn diese Makros oder Autostart-Makros enthalten.

3.18.2.4 LTE-Unterstützung

Die bisherigen USB-Sticks für die Internetanbindung über UMTS laufen aus. Es werden nun LTE-fähige Sticks angeboten.

Die Konfigurationsmaske für die Internetanbindung über Mobilfunk wurde um die Anzeige des Mobilfunkproviders und um eine Auswahlmöglichkeit für den Mobilfunkstandard erweitert.

3.18.2.5 Auswahl des IKEv2-Modus in IPsec-Verbindungen

In IPsec-Verbindungen vom Typ "Server" und "Client" kann nun der IKEv2-Modus vorgegeben werden.

3.18.3 Änderung

3.18.3.1 Schlüssel- und Zertifikatsmanagement

RSA-Schlüsselpaare für Serverdienste wie VPN, Reverse-Proxy, E-Mail-Server und Administrationsoberfläche wurden bisher in den jeweiligen Menüs dieser Dienste administriert. Ab sofort werden die Schlüsselpaare zentral im Menü "System > Zertifikatsverwaltung > Schlüsselbund" abgelegt. In den Menüs der Dienste wird ausgewählt, welcher der Schlüssel aus dem Schlüsselbund genutzt werden soll.

Auf Cluster-Systemen wird solange keine Synchronisierung der RSA-Schlüsselpaare mehr durchgeführt, bis beide Cluster-Knoten aktualisiert wurden.

Der spezielle Schlüssel "DUMMY" dient als Platzhalter. Er wird in der Grundkonfiguration verwendet, solange noch kein richtiges Schlüsselpaar zur Verfügung steht. Ferner kommt er zum Einsatz, wenn der private Schlüssel eines Schlüsselpaars fehlt, was z.B. nach einem Hardwaretausch der Fall ist, bevor die Backups der Schlüsselpaare eingespielt oder neue Schlüssel ausgestellt wurden. Beachten Sie bitte, dass private Schlüssel nach wie vor nicht Bestandteil des System-Backups sind sondern separat in kennwortgeschützten Dateien gesichert werden müssen.

Im Zuge der Umstellung wurde der Prozess zur Beantragung von Kaufzertifikaten überarbeitet. Unter anderem lassen sich Zertifikatsanfrage und Zertifikat jetzt alternativ per Copy-und-Paste übertragen und Zertifikate könne auch im DER-Format hochgeladen werden.

3.18.3.2 Re-keying in IPsec-Verbindungen

In IPsec-Verbindungen vom Typ "Client" und in passiven "Server"-Verbindungen wurde kurz vor Ablauf eines Sitzungsschlüssels ggf. ein re-keying initiiert. Die Verbindungen sind jetzt komplett passiv.

3.18.4 Update

3.18.4.1 Zahlreiche Softwarepakete

Neben dem Linux-Kernel und den Virenscannern von Avira und F-Secure wurden diverse System-Bibliotheken und Programme aktualisiert.

3.18.4.2 URL-Filter Datenbank

3.18.4.3 IDS/IPS-Signaturen für Systeme ohne Pflegevertrag

3.19 Version 7.0-2-6

3.19.1 Sicherheitskritisch

3.19.1.1 Aktualisierung des Linux-Kernels und der Systembibliothek glibc

Der Schutzmechanismus, mit dem die verschiedenen Speicherbereiche eines Programmes voneinander getrennt werden, lässt sich umgehen. Dies ermöglicht das Ausführen von eigenem Code oder das Ausweiten der Berechtigungen. Mit dem Update werden entsprechende Angriffe erschwert.

3.19.1.2 RAR-Entpacker

Mit Hilfe eines manipulierten RAR-Archives konnte ein Angreifer den im E-Mail-Virenscan eingesetzten RAR-Entpacker dazu bringen, im Rahmen der Berechtigungen eigenen Code auszuführen.

3.19.2 Bugfix

3.19.2.1 OpenVPN

Mit Hilfe von speziellen Datenpaketen konnte ein Angreifer den OpenVPN-Server zum Absturz bringen.

3.19.2.2 E-Mail Dateianhangsfilter

In der Administrationsoberfläche wurden Dateinamen mit ausländischen Zeichensätzen nicht korrekt angezeigt. In den Benachrichtigungsmails betraf dies neben dem Dateinamen auch den Betreff.

Um den Text der Benachrichtigungsmails zu vereinfachen, sind die Kopfzeilen der Original-Mail nicht mehr Bestandteil des Textes sondern werden als Anhang zugeordnet.

3.19.2.3 SPAM-Ordner E-Mail-Report

Im täglichen E-Mail-Report, der neue E-Mails im SPAM-Ordner auflistet, wurden Absendernamen und Betreff möglicherweise abgeschnitten. Bei Verwendung von ausländischen Zeichensätzen war die Anzeige nicht korrekt.

3.19.3 Neu

3.19.3.1 Reverse-Proxy-Option für Quarantänebereich des Dateianhangsfilters

Seit 7.0-2.0 kann der Administrator den Empfängern ermöglichen, unter bestimmten Voraussetzungen selbst auf gefilterte E-Mails oder Anhänge zugreifen zu können. Über einen neuen Schalter können diese Zugriffe nun auch im Reverse-Proxy freigegeben werden, falls von außen ein Zugriff auf die Quarantäne notwendig ist.

3.19.3.2 Monitoring für SSH-TCP-Forwarding

Auf einem neuen Reiter im Menü "Monitoring > Netzwerk > Status" werden jetzt Verbindungen mit dem SSH-TCP-Forwarder angezeigt.

3.20 Version 7.0-2-5

3.20.1 Sicherheitskritisch

3.20.1.1 Windows-Freigaben

Bei aktivierten Windows-Freigaben konnte ein Client eine Bibliothek hochladen und zur Ausführung bringen. Wenn der Dienst "Windows-Freigaben" nicht läuft, was der Grundeinstellung entspricht, ist das System nicht angreifbar.

3.20.2 Bugfix

3.20.2.1 NTLM-Authentifzierung und Mitgliedschaft in der Windows-Domäne

Bei NTLM basierter Proxy-Authentifizierung gab es mit der in Version 7.0-2.2 installierten neuen Samba-Version Probleme. Teils wurden nur viele Log-Meldungen erzeugt, auf anderen Sytemen musste hingegen der Dienst "Mitgliedschaft in Windows Domäne" regelmäßig neu gestartet werden.

Bitte erstellen Sie auf betroffenen Sytemen nach Abschluss des Updates im Menü "Module > Web-Proxy > Einstellungen" auf dem Reiter "NTLM-Anmeldung" das Domänen-Konto neu. Sollte bei "IP-Adresse des ActiveDirectory-Servers" anstatt einer IP der Name der Windows-Domäne konfiguriert sein, ändern Sie diesen bitte in die IP-Adresse eines Ihrer Domain-Controller ab.

3.21 Version 7.0-2-4

3.21.1 Sicherheitskritisch

3.21.1.1 IPSec-Server

Mit manipulierten Zertifikaten ließ sich der IPsec-Server zum Absturz bringen oder sogar Programmcode ausführen.

3.21.1.2 Intrusion-Prevention und F-Secure Antivirus

Seit 27.04.2017 wurden teilweise die Updates des F-Secure Virenscanners durch die Intrusion-Prevention blockiert. Systeme mit Pflegevertrag und automatischem Update der IDS/IPS-Signaturen haben am 28.04.2017 Signaturen erhalten, in denen das Problem behoben wurde. Für alle anderen Systeme werden die Signaturen mit diesem Update aktualisiert.

3.21.2 Update

3.21.2.1 Aktualisierung des Linux-Kernel

3.22 Version 7.0-2-3

3.22.1 Sicherheitskritisch

3.22.1.1 Intrusion-Detection / -Prevention

Mit manipulierten, fragmentierten Paketen konnten das IDS/IPS dazu gebracht werden, falsche Pakete bei der Reassemblierung des Datenstroms zu benutzen.

3.22.1.2 IPsec CRL

Zertifikatssperrlisten wurden vom IPsec-Server nicht geladen.

3.22.2 Bugfix

3.22.2.1 Autostart des Dienstes "weitere Server"

Auf dem Cluster Master und nach dem Einspielen eines System-Backups wurde das automatische Starten nach Reboots für "weitere Server" nicht aktiviert.

3.22.2.2 Webmail über Reverse-Proxy

Das Versenden von E-Mails im Webmailer schlug fehl, wenn der Zugriff über den Reverse-Proxy erfolgte.

3.22.2.3 Firewall-Regeln mit vielen Adressen

In Version 7.0-2.2 kam es beim Laden von Firewall-Regeln mit sehr vielen IP-Adressen zu einem Fehler. Die Regeln wurden daraufhin in einem zeitaufwändigen Verfahren schrittweise geladen, was zu temporären Zugriffsproblemen führen konnte.

3.23 Version 7.0-2-2

3.23.1 Sicherheitskritisch

3.23.1.1 Web-Proxy

Ein Fehler bei der Verarbeitung bedingter Anfragen ermöglichte es internen Angreifern, Zugriff auf die Sitzungen anderer Nutzer und damit potentiell auf vertrauliche Daten zu erlangen.

3.23.1.2 Filterung von eingehenden E-Mails mit Absenderadresse aus der eigenen Domain

Das Update behebt mehrere Möglichkeiten, diese in 7.0-1.1 neu eingeführten Filter zu umgehen. So wurden z.B. bislang nur die E-Mail-Adresse, nicht jedoch der Text-Teil des From-Headers untersucht und nur der erste From-Header geprüft.

Der Sender-Header wird ab sofort ebenfalls geprüft.

3.23.1.3 Windows-Dienste

Im Samba-Server wurden diverse Sicherheitsprobleme behoben, die nach unserer Auffassung jedoch nicht relevant sein dürften. Vorsichtshalber stellen wir dennoch ein Update zur Verfügung.

3.23.2 Neue Funktionen

3.23.2.1 Protokollierung auf Syslog-Server

Kostenpflichtige Funktion und nur auf Systemen mit Software-Updatevertrag verfügbar.

Der Inhalt der meisten Log-Dateien kann jetzt in Kopie auf einen Syslog-Server gesendet werden.

3.23.2.2 Eingabe von IP-Bereichen

In der Administrations-Oberfläche lassen sich nun an vielen Stellen neben einzelnen IP-Adressen und Netzwerken auch IP-Bereich wie z.B. "192.168.0.100-192.168.0.120" eingeben.

3.23.3 Bugfix

3.23.3.1 Cluster mit Fallback

Das Verhalten von Cluster-Master-Knoten, die zugleich über ein Fallback auf eine zweite Internet-Leitung verfügen, wurde überarbeitet. Wenn der Netzwerk-Link auf der primären Internet-Leitung verloren geht, erfolgt kein Wechsel auf den Backup-Knoten mehr. Stattdessen erfolgt ein Fallback auf die zweite Internet-Leitung.

3.23.3.2 Anzeige von Dateianhängen in der E-Mail Quarantäne

Vereinzelt wurden Anhänge nicht angezeigt, wenn deren Dateinamen auf bestimmte Weise kodiert waren.

3.23.3.3 Anzeige der Schnittstellen-Tabelle

Auf Hyper-V Systemen und manchen VDSL-Systemen wurde die Schnittstellen-Tabelle im Monitoring nicht angezeigt.

3.24 Version 7.0-2-1

3.24.1 Neue Funktionen

3.24.1.1 Abweisen von E-Mails mit unerwünschten Dateianhängen

Bei der Filterung von Dateianhängen steht nun eine zusätzliche Option zur Verfügung, bei der E-Mails mit unerwünschten Anhängen nicht unter Quarantäne gestellt, sondern gar nicht erst angenommen werden.
Diese Option ist nicht geeignet für Systeme, die eingehende E-Mails von einem POP- oder IMAP-Server abholen.

3.24.2 Bugfix

3.24.2.1 Import-Funktion für Konfigurationstabellen

Mit der neuen Import-Funktion aus 7.0-2.0 gab es noch ein paar Schwierigkeiten. Der Import funktioniert nun auch mit Chrome und der doppelte Import bei Verwendung des Internet-Explorers wurde behoben. Teilweise wurde die letzte Zeile des Imports fälschlicherweise als fehlerhaft beanstandet. Schließlich ist der Importvorgang jetzt toleranter bezüglich des Dateiformats, so dass sich die Import-Dateien nun mit den meisten Editoren bearbeiten lassen sollten.

3.24.2.2 DSL-Einwahl nach Neustart

An manchen DSL-Anschlüssen ging nach einem Neustart des Systems die DSL-Verbindung nicht online, wenn die DSL-Schnittstelle auch für IPsec-VPN genutzt wurde.

3.24.2.3 Backup auf NetAPP Windows-Freigabe

Das Backup schlug fehl, sofern in der NetAPP NTLMv2-Signed aktiviert ist.

3.24.2.4 Speicherleck im Reverse-Proxy

Testmöglichkeit

Überzeugen Sie sich zwei Wochen lang von unseren Produkten und Leistungen – ganz ohne Verpflichtung und völlig kostenfrei.

Kompetente Beratung

Oft ist die gewünschte Lösung einfacher und effizienter zu realisieren als erwartet.
Sprechen Sie mit uns über Ihre Anforderungen.
Gemeinsam finden wir den richtigen Weg.

Erreichbarkeit

Ihren persönlichen Ansprechpartner erreichen Sie ohne Umwege über seine direkte Durchwahl.

Vorabaustausch

Im Falle einer Störung senden wir Ihnen umgehend vorab ein vorinstalliertes und voll funktionstüchtiges Gerät zu.

Hotline

Bei allen technischen Fragen können Sie sich auf ein erfahrenes Support-Team verlassen.

XnetSolutions

Benzstraße 32, 71083 Herrenberg/Germany
Telefon +49 (0) 7032 955 96-0
Telefax +49 (0) 7032 955 96-25
info@xnetsolutions.de
www.xnetsolutions.de