MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Datenschutz versus Sicherheit: Ab wann Sie TLS-Verbindungen aufbrechen sollten

11.07.2022 08:00 Uhr Stefan Hessel, Christoph Puppe

Die meiste Schadsoftware kommt über TLS-verschlüsselte Downloads ins Unternehmen. Diese Verbindungen lassen sich aufbrechen und scannen – aber ist das erlaubt?

Nicht nur Ransomware kommt fast immer per TLS-geschütztem Download, auch die Command-and-Control-Server von Ransomware und anderen Angriffswerkzeugen kommunizieren meist über HTTPS. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt im IT-Grundschutz-Kompendium, auf dem Web-Proxy alle Verbindungen aufzubrechen und auf Malware zu untersuchen. Auch die DSGVO fordert in § 32 den Schutz der Daten, und da Ransomware oft Daten veröffentlicht, ist diese Maßnahme zum Schutz der personenbezogenen Daten und der Geschäftsgeheimnisse unbedingt erforderlich.

Da allerdings bei der Untersuchung der eigentlich mit TLS verschlüsselten Verbindungen die Inhalte der Websessions sichtbar werden, sind auch die Datenschutzanforderungen und Mitarbeiterrechte zu beachten.

MEHR ZU: UNTERNEHMENSSICHERHEIT

Security: Wie der Cyberrisiko-Check kleine Unternehmen schützen soll [1]

Sliver – ein OS-Framework für Red Teams [2]

TLS-Verschlüsselung: Datenschutz versus Schutz vor Malware [3]

IT-Sicherheitstests: Vom Schwachstellenscan zum automatisierten Pentesting [4]

Ukrainekrieg: Auswirkungen auf die IT-Sicherheit in Deutschland [5]

IT-Versicherungsschutz für kleine Unternehmen und Freelancer [6]

Security: Ransomware-Angriffsmuster und wie man sich vor ihnen schützt [7]

Security: So laufen Ransomware-Angriffe heute ab [8]

IT-Recht: Sicherheitsanforderungen und Rechtsfragen zu Ransomware-Attacken [9]

Manche Organisationen entscheiden sich deswegen gegen die Suche nach Schadsoftware am zentralen Proxy. Dieser Artikel zeigt die Anforderungen des Datenschutzes, mögliche Vorkehrungen und die Risiken eines Verzichts auf die Umsetzung der BSI-Anforderungen.

IX-TRACT

- Verschlüsselte Netzwerkverbindungen sollen die Inhalte vor dem Zugriff Dritter schützen.
- Aber auch Malware nutzt oft TLS-geschützte Downloads für den Weg in Unternehmensnetze oder die Kommunikation mit Command-and-Control-Servern.
- Sicherheitsmaßnahmen, die gemäß den Empfehlungen des BSI den verschlüsselten Datenverkehr inspizieren, können mit Datenschutzanforderungen ins Gehege kommen.
- Mit geeigneten Vorkehrungen lassen sich Sicherheitsmaßnahmen BSI- und datenschutzkonform ergreifen, ohne Mitarbeiterrechte mehr als nötig einzuschränken.

Risiko Drive-by-Download und Phishing

Jeden Tag werden Webseiten zum Zweck übernommen, die Besucher mit Schadsoftware zu infizieren. Hunderttausende oder Millionen Seiten warten nur darauf, dass ein verwundbarer Browser sie besucht oder dass der Nutzer den Klick macht, der zur Installation der Schadsoftware führt. Etwas gezielter ist hier Phishing: Die Benutzer erhalten eine E-Mail oder Chatnachricht mit einem Link zu einer Webseite mit der Schadsoftware. Die Angreifer sind hier sehr raffiniert, tarnen die Links gut oder machen den Nutzern Angst vor Haftbefehlen und Ähnlichem, damit sie auch wirklich klicken. Der Server, der dann die Schadsoftware ausliefert, erkennt automatisch das Betriebssystem und den Browser. So kann er einen erfolgversprechenden Angriff ausführen und die passende Software schicken.

Um die Relevanz einer Sicherheitsmaßnahme einschätzen zu können, muss man das damit abgewehrte Risiko kennen. Und es gibt wohl keines, das höher zu bewerten ist als Schadsoftware – sei es als initialer Angriffsvektor oder als Teil eines über andere Wege ausgeführten Angriffs.

Laut **Verizon Breach Report 2021 [10]** spielt Malware in mehr als 80 Prozent der Sicherheitsvorfälle eine Rolle. Und wie kommt diese auf die IT-Systeme der Opfer? In fast allen Fällen über einen TLS-verschlüsselten Download. Auch nutzt Schadsoftware meist eine mit TLS verschlüsselte HTTPS-Verbindung zur Kommunikation mit den Angreifern. Wenn es also gelingt, diese Downloads und die Kommunikation zu unterbinden, lassen sich die meisten Einbrüche verhindern oder zumindest deren Auswirkungen stark reduzieren.

[11]

Antivirensoftware mit beschränktem Nutzen

Ein notwendiger Schutz ist es, Downloads genau wie Datenträger, E-Mails und Chats auf Malware zu untersuchen. Der Proxy kann die Downloads allerdings nur dann untersuchen, wenn er die HTTPS-Verbindung entschlüsselt und so Einblick in den Datenstrom hat. Wer hier auf eine Lösung für den Schutz des Endgerätes setzt, hat sicherlich schon viel gewonnen, da sie in den Browser hineinsehen kann – zumindest solange der Browser selbst nicht verwundbar ist.

Die meiste Schadsoftware tarnt sich durch stete Veränderung vor den üblichen signaturbasierten AV-Scannern. Oft vergehen Tage, bis diese eine neue Variante einer bekannten Schadsoftware zuverlässig erkennen. Daher dürfen keine Dateitypen von der Untersuchung ausgenommen werden. Neue Ansätze bei der Suche nach Schadsoftware mit Maschinenlernen und Überwachung der Prozesse auf unübliches Verhalten (Behavior Engines) funktionieren auf dem Endgerät, und zumindest ML hilft auch auf dem Proxy, neue Varianten und komplett neue Malware zu erkennen. Beides hat die Erkennungsrate stark verbessert.

Auch Sandboxing, bei dem eine ausführbare Datei erst in einer virtuellen Maschine überwacht gestartet wird, bringt einiges. Leider ist dies sehr zeitaufwendig. Oft nutzen die Antivirusprodukte für das Sandboxing Cloud-Dienste des Herstellers, was nicht jeder Kunde möchte, da dies auch vertrauliche Dateien an den Anbieter überträgt.

Auch wenn die Virenscanner nicht jede Malware zuverlässig entdecken und sie auch selbst verwundbar sein können, ist der Einsatz notwendig. Sie erhöhen zumindest den Aufwand für die Angreifer und alle zusätzlichen Kosten für die Angreifer sind ein Schritt in die richtige Richtung.

Zusammenfassend kann man sagen, dass die Vorgaben des BSI sehr sinnvoll sind, denn nur ein zentraler Proxy, der auch in die HTTPS-Verbindungen Einsicht hat, kann diesen Angriffsweg blockieren. Es gilt hier natürlich auch, dass auch diese Blockade nicht absolut ist. Sie erhöht aber den Aufwand für die Angreifer und reduziert so die Eintrittshäufigkeit. In der Kombination mit einer guten Schutzsoftware auf den Geräten ist es allerdings die beste Maßnahme zur Verbesserung des Schutzes und aus Sicht der IT-Sicherheit unbedingt notwendig.

Datenschutzaspekte für die Praxis

Dass es technisch sinnvoll oder gar notwendig ist, TLS-Verbindungen zu entschlüsseln, führt nicht dazu, dass eine entsprechende Praxis ohne Weiteres rechtlich zulässig ist. Beim Entschlüsseln von TLS-Verbindungen werden in aller Regel personenbezogene Daten der Beschäftigten verarbeitet. Betroffen sind neben Inhaltsdaten wie Namen oder Eingaben auf Webseiten auch Metadaten, etwa IP-Adressen. Insbesondere wenn Beschäftigte den Internetzugang – und sei es auch nur gelegentlich – privat nutzen, können sich daher datenschutzrechtliche Herausforderungen ergeben.

In der Vergangenheit vertraten hierzu insbesondere Datenschutzaufsichtsbehörden und einige juristische Fachautoren die Auffassung, dass Arbeitgeber, die eine Privatnutzung des Internets gestattet hatten, das Fernmeldegeheimnis des Telekommunikationsgesetzes (TKG) zu beachten hätten. Dies hatte zur Folge, dass Arbeitgeber nur in den nach dem TKG vorgesehenen engen Ausnahmefällen TLS-Entschlüsselung einsetzen durften und dass die Datenschutzvorschriften des TKG sowie des Telemediengesetzes (TMG) Anwendung fanden. Aufgrund der damaligen Zweifel war es für Unternehmen deswegen sinnvoll, eine Einwilligung der Beschäftigten in die Entschlüsselung von TLS-Verbindungen einzuholen.

Inzwischen wurde die langwierige Diskussion um die rechtliche Zulässigkeit durch das Inkrafttreten des neuen Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG) entschärft. Die Regelungen zum Fernmeldegeheimnis und Datenschutz wurden aus dem TKG und TMG gestrichen und in abgewandelter Form in das neue TTDSG überführt. Dieses spricht im Wortlaut nicht mehr von der Verpflichtung jedes Diensteanbieters zur Wahrung des Fernmeldegeheimnisses, sondern führt die Verpflichteten einzeln auf. Arbeitgeber sind dort nicht genannt und nach heute herrschender Meinung auch nicht durch andere Kategorien von Verpflichteten miterfasst. Ob sich diese Einschätzung auch bei den Datenschutzaufsichtsbehörden und den Gerichten durchsetzt, muss sich freilich noch zeigen.

Ist das Fernmeldegeheimnis nicht anwendbar, sind zumindest die Regelungen der Datenschutz-Grundverordnung (DSGVO) zu beachten. Nach dieser ist das Verarbeiten personenbezogener Daten nur zulässig, wenn es dafür eine Rechtsgrundlage gibt. Beim Entschlüsseln von TLS-Verbindungen kommt als solche insbesondere das berechtigte Interesse des Arbeitgebers an der Gewährleistung von IT-Sicherheit in Betracht. Dieses muss jedoch das Interesse der Beschäftigten am Schutz ihrer Privatsphäre überwiegen. Da ein Entschlüsseln von TLS-Verbindungen technisch sinnvoll ist und die Erwägungsgründe der DSGVO explizit auf die Gewährleistung der Netz- und Informationssicherheit Bezug nehmen, lassen sich insoweit für Arbeitgeber gute Argumente finden.

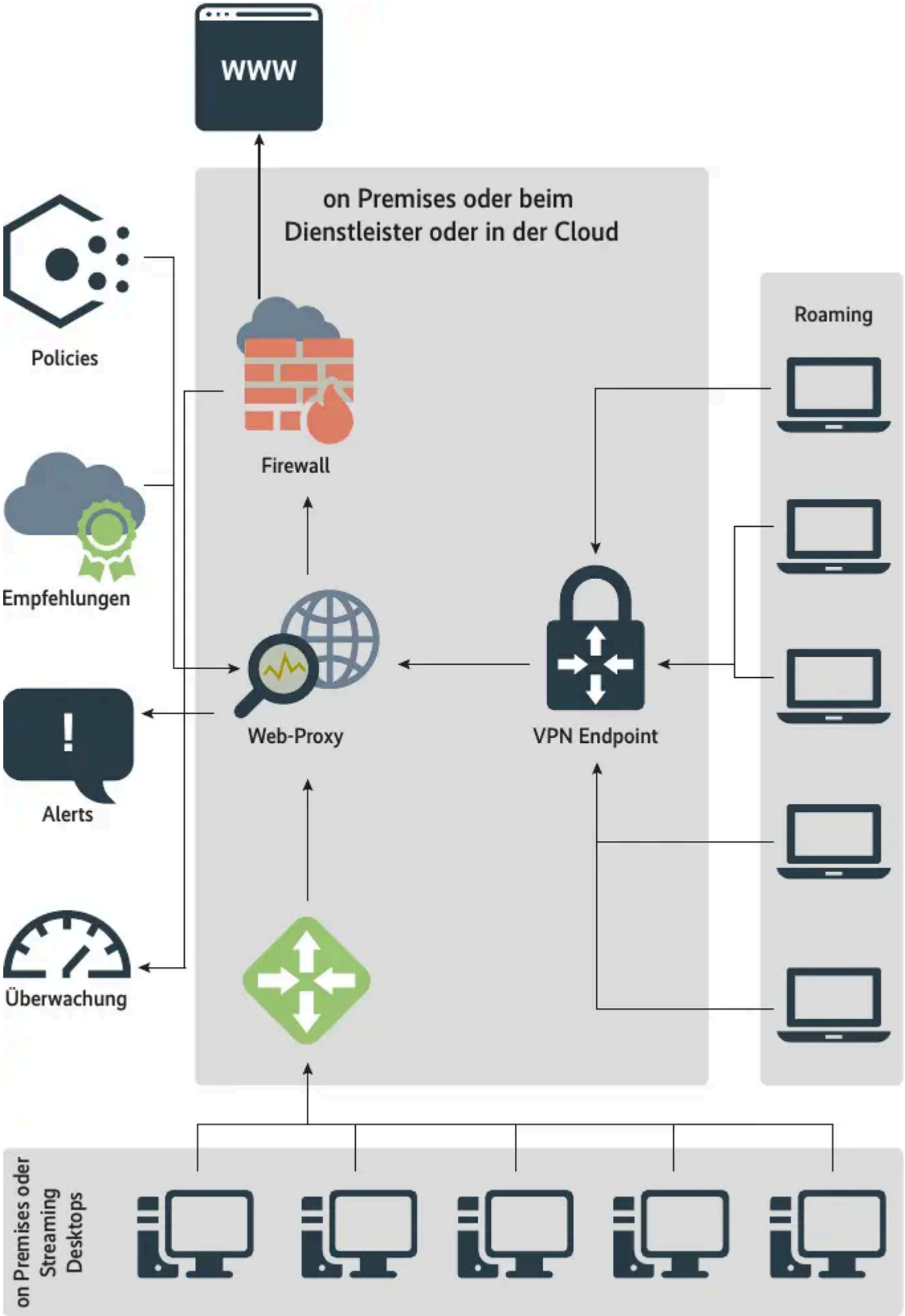
Dies gilt insbesondere, wenn eine Privatnutzung des Internetzugangs nicht gestattet ist. Wenn doch, sollte die Firma aus Gründen der Rechtssicherheit zusätzliche Maßnahmen ergreifen. Die private Nutzung gilt schon als gestattet, wenn sie nur gelegentlich stattfindet und toleriert wird. Rechtssicher ist die explizite Einwilligung der Mitarbeiter oder eine Betriebsvereinbarung zur privaten Internetnutzung – beides jeweils mit dem Hinweis auf die Sicherheitsmaßnahmen. Dann ist der Benutzer informiert und willigt mit der privaten Nutzung des dienstlichen Internetanschlusses in die Kontrolle der Inhalte ein.

Die Organisation ist allerdings immer verpflichtet, den Zugang zu den Protokolldateien des Web-Proxys stark zu reglementieren. Nur ein kleiner Personenkreis darf darauf zugreifen. Und Auswertungen des Verhaltens von Mitarbeitern sind immer mit dem Betriebsrat, dem Vorgesetzten und dem Datenschutzbeauftragten abzusprechen. Wer sicherstellen will, dass keine unerlaubte Auswertung stattfindet, kann den Betrieb des Web-Proxys an einen Dienstleister auslagern. Dieser sichert dann vertraglich zu, dass nur berechtigte Personen des Auftraggebers Einsicht erhalten und Auswertungen anfordern dürfen.

Technische Realisierung

Die zentrale Bedingung für den Erfolg dieser Maßnahme ist das Filtern aller ausgehenden Verbindungen von allen Geräten. Wenn die Geräte beliebige Internetverbindungen aufbauen können, ist der zentrale Proxy schnell umgangen. Paketfilter zwischen internen Netzen und auch auf den mobilen Geräten müssen die Nutzung des zentralen Proxys für jede Verbindung erzwingen. Das sollte auch für Server gelten, denn auch die Angriffe gegen Server benötigen in den meisten Fällen Verbindungen zum Internet, die es zu verhindern gilt.

Ist der zentrale Proxy so zur Pflicht gemacht, kann er die HTTPS-Verbindung selbst beantworten. Er muss gegenüber dem Endgerät behaupten, dass er der eigentliche Server ist. Dafür erzeugen die Proxys ein temporäres Zertifikat, das sie mit einem eigenen Wurzelzertifikat unterschreiben. Die Endgeräte müssen diesem Wurzelzertifikat daher vertrauen und es ist auf allen Endgeräten zu installieren. Der Proxy baut dann selbst eine Verbindung zum eigentlichen Zielserver auf. Dabei ist zu beachten, dass der Proxy ein gefälschtes Zertifikat erkennt und die Verbindung ablehnt. Auch sollte er nur aktuelle TLS-Versionen akzeptieren.



So könnte ein typisches Set-up eines zentralen Webgateways mit Überwachung, Benachrichtigungen, automatisierten Empfehlungen und Richtlinien für die Benutzung aussehen.

Mit diesem Ansatz sind allerdings auch technische Herausforderungen verbunden. Das Einfachste ist noch, das Wurzelzertifikat zu verteilen. Allerdings hat manche mobile App für iOS und Android die Angewohnheit, sich das verwendete Zertifikat zu merken und sich zu beschweren, wenn es sich ändert. Hier muss der Betreiber Ausnahmen einstellen, die der Proxy ohne Öffnen des TLS weiterleitet. Das werden bei größeren Organisationen gerne mal mehrere Hundert. Browser konnten dies früher auch mit **HTTP Public Key Pinning (HPKP) [12]**, aber das wird seit Jahren nicht mehr empfohlen und von modernen Browsern auch nicht mehr unterstützt. Beispiele für Apps, die dies nutzen, sind Banking- und Versicherungs-Apps. Aber auch Zahlungssystemanbieter und andere sicherheitsbewusste Firmen nutzen es. Nur beruflich genutzte Apps sollten Ausnahmen erhalten, private Geräte sollten im internen Netz und WLAN keinen Zugang bekommen.

Bei Remote-Nutzern kommt gerne der Einwand, dass das Internet so langsam ist, wenn der Traffic erst über das VPN in die Zentrale geleitet wird und dann über den Proxy fließt. Das ist leider kaum zu vermeiden. Hilfreich ist es hier, Verbindungen zu Servern, die der Nutzer oft und viel benötigt – etwa Cloud-Dienste für Büroanwendungen, Backups und Dateifreigabe (O365, Dropbox et cetera) sowie Videokonferenzen –, auf dem Endgerät direkt ins Internet zu leiten. Dies vermeidet den Umweg über VPN und Proxy. Dann muss allerdings sichergestellt sein, dass diese Seiten keine Schadsoftware verteilen, indem dort beispielsweise der AV-Schutz und die Filterliste für bestimmte Dateien aktiv sind.

Fazit

Malware, Schadsoftware, Ransomware sind die drei apokalyptischen Reiter der IT. Die Malware-Risiken sind real, täglich grüßt der Sicherheitsvorfall. Bei allen Anbietern von Sicherheitsvorfallbehandlung ist die Warteliste lang. Downloads auch per TLS auf Schadsoftware zu untersuchen ist daher – wie vom BSI empfohlen – eine Notwendigkeit. Wenn die Geschäftsführung das Risiko trägt, ist dies gemäß KontraG auch eine mangelhafte Risikovorsorge. Der Datenschutz der Mitarbeiter muss allerdings beachtet werden, die Mitarbeiter müssen darüber informiert sein und der Zugang zu den Traffic-Protokollen ist stark zu regulieren. Dann lässt sich das Untersuchen der verschlüsselten Verbindungen DSGVO- und BSI-konform betreiben und gegenüber dem Betriebsrat auch als notwendige Sicherheitsmaßnahme vertreten.

Exkurs: BSI-Vorgaben

Auszug aus den BSI-Vorgaben

Das BSI hat klare Vorgaben für den Schutz vor Schadsoftware. Die Standardanforderung ist immer umzusetzen und die erhöhte Anforderung nur dann, wenn die Risikoanalyse ergeben hat, dass das zugrunde liegende Risiko nicht bereits durch die Basis- und Standardanforderungen ausreichend reduziert wurde. Bei den Standardanforderungen verwendet das BSI im IT-Grundschutz-Kompendium das Modalverb SOLLTE, aber sie sind für eine Standardabsicherung Pflicht, sofern nicht eine andere Maßnahme das Risiko ausreichend reduziert oder die Geschäftsleitung das Risiko tragen möchte. Die Standardabsicherung ist auch die Grundlage für eine Zertifizierung ISO 27001 nach Grundschutz.

Standardanforderung NET.3.2.A21: Temporäre Entschlüsselung des Datenverkehrs

Verschlüsselte Verbindungen in nicht vertrauenswürdige Netze SOLLTEN temporär entschlüsselt werden, um das Protokoll zu verifizieren und die Daten auf Schadsoftware zu prüfen. Hierbei SOLLTEN die rechtlichen Rahmenbedingungen beachtet werden. Die Komponente, die den Datenverkehr temporär entschlüsselt, SOLLTE unterbinden, dass veraltete Verschlüsselungsoptionen und kryptografische Algorithmen benutzt werden. Der eingesetzte TLS-Proxy SOLLTE prüfen können, ob Zertifikate vertrauenswürdig sind. Ist ein Zertifikat nicht vertrauenswürdig, SOLLTE es möglich sein, die Verbindung abzuweisen. Eigene Zertifikate SOLLTEN nachrüstbar sein, um auch „interne" Root-Zertifikate konfigurieren und prüfen zu können. Vorkonfigurierte Zertifikate SOLLTEN überprüft und entfernt werden, wenn sie nicht benötigt werden.

Erhöhte Anforderung NET.3.2.A28: Zentrale Filterung von aktiven Inhalten

Aktive Inhalte SOLLTEN gemäß den Sicherheitszielen der Institution zentral gefiltert werden. Dafür SOLLTE auch der verschlüsselte Datenverkehr entschlüsselt werden. Die erforderlichen Sicherheitsproxies SOLLTEN es unterstützen, aktive Inhalte zu filtern.

Standardanforderung DER.1.A10: Einsatz von TLS-/SSH-Proxies

An den Übergängen zu externen Netzen SOLLTEN TLS-/SSH-Proxies eingesetzt werden, welche die verschlüsselte Verbindung unterbrechen und es so ermöglichen, die übertragenen Daten auf Malware zu prüfen. Alle TLS-/SSH-Proxies SOLLTEN vor unbefugten Zugriffen geschützt werden. Auf den TLS-/SSH-Proxies SOLLTEN sicherheitsrelevante Ereignisse automatisch detektiert werden. Es SOLLTE eine organisatorische Regelung erstellt werden, unter welchen datenschutzrechtlichen Voraussetzungen die Log-Daten manuell ausgewertet werden dürfen.

Stefan Hessel ist Senior Associate und Co-Head der Digital Business Unit bei Reusch Rechtsanwälte in Saarbrücken. Er berät nationale und internationale Unternehmen zu Datenschutz, Cybersicherheit und IT-Recht.

Christoph Puppe ist Managing IT Security Architect und Auditteamleiter für ISO 27001 nach Grundschutz bei SVA System Vertrieb Alexander GmbH, Mitautor des Grundschutz-Kompendiums und ehemaliger Penetrationstester.

(**avr [13]**)

URL dieses Artikels:

`https://www.heise.de/-7165191`

Links in diesem Artikel:

[1] `https://www.heise.de/hintergrund/Security-Wie-der-Cyberrisiko-Check-kleine-Unternehmen-schuetzen-soll-9162982.html`

[2] `https://www.heise.de/hintergrund/Silver-Profiwerkzeug-fuer-Angriffssimulationen-in-der-Praxis-7220149.html`

[3] https://www.heise.de/hintergrund/Datenschutz-versus-Sicherheit-Ab-wann-Sie-TLS-Verbindungen-aufbrechen-sollten-7165191.html

[4] https://www.heise.de/hintergrund/IT-Sicherheitstests-Vom-Schwachstellenscan-zum-automatisierten-Pentesting-6670831.html

[5] https://www.heise.de/hintergrund/Ukrainekrieg-Auswirkungen-auf-die-IT-Sicherheit-in-Deutschland-6668405.html

[6] https://www.heise.de/hintergrund/IT-Versicherungsschutz-fuer-kleine-Unternehmen-und-Freelancer-6489094.html

[7] https://www.heise.de/ratgeber/Security-Ransomware-Angriffsmuster-und-wie-man-sich-vor-ihnen-schuetzt-6457415.html

[8] https://www.heise.de/ratgeber/Security-So-laufen-Ransomware-Angriffe-heute-ab-6457906.html

[9] https://www.heise.de/hintergrund/IT-Recht-Sicherheitsanforderungen-und-Rechtsfragen-zu-Ransomware-Attacken-6474409.html

[10] https://www.verizon.com/business/resources/reports/dbir/2021/

[11] https://www.heise.de/ix/

[12] https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning

[13] mailto:avr@ix.de