viprinet®

SICHERHEIT VON UNTERNEHMENSNETZWERKEN IM ZEITALTER DER DATENÜBERWACHUNG

ZUSAMMENFASSUNG

Seit den Enthüllungen durch Edward Snowden, die gezeigt haben, in welchem Ausmaß und mit welcher Selbstverständlichkeit Geheimdienste jeglichen Internetverkehr überwachen und dadurch unbescholtene Bürger gesetzeswidrig zu Verdächtigen machen, ist erstmals der Schutz von Unternehmensdaten branchenübergreifend in den Fokus gerückt. Während zuvor Datensicherheit für Unternehmen eine nette Beigabe war und oftmals vernachlässigt wurde, sehen sie nun immer mehr Firmen als zentralen Bestandteil ihrer Anbindungslösung. Allerdings hilft es nicht, das erstbeste Angebot für Datensicherheit zu wählen, denn zu oft stehen hinter diesen Angeboten wiederum die Geheimdienste, die eigentlich ausgesperrt werden sollen.

Dieses Whitepaper richtet sich an alle Personen, die die Datensicherheit eines Unternehmens zu verantworten haben. Es liefert Hintergrundwissen, wie sich Geheimdienste unbemerkt Zugang zu praktisch allen digitalen Daten verschaffen können und erklärt, worauf man achten muss, wenn man seine Daten wirklich schützen möchte. Außerdem nennt es verfügbare Lösungsmöglichkeiten.

EINLEITUNG

Um überhaupt ein derartiges Ausmaß an Datenüberwachung zu erreichen, wie von Edward Snowden beschrieben – 160.000 abgegriffene E-Mails und hunderte Seiten lange Chatmitschriften sowie Katalogisierung des Alltags von über 10.000 Personen und das allein in den USA[1] – braucht es ein ausgeklügeltes System, das aus zwei Maßnahmen besteht: sich unbemerkt Zugang verschaffen und Verschlüsselungsmechanismen aushebeln.

DATENKRAKEN AN IHRER HINTERTÜR

Unbemerkten Zugang zu vertraulichen Daten erreicht man am besten mit eingebauten Hintertüren, sogenannten „backdoors". So bewilligt etwa das US-amerikanische FISA Gericht („Foreign Intelligence Surveillance Act") ständig Überwachungsanfragen von der NSA, obwohl es eigentlich dafür zuständig ist, diese Anfragen auf ihre absolute Notwendigkeit zu prüfen[2], und mit National Security Letters – Anordnungen ohne richterlichen Beschluss – kann das FBI Daten von Telefon- und Netzbetreibern fordern, oft ohne dass diese ihre Kunden darüber in Kenntnis setzen dürfen[3].

1 Martin Holland: „NSA-Skandal: Die allermeisten Überwachten sind keine Zielpersonen." In: heise online. URL: http://www.heise.de/newsticker/meldung/NSA-Skandal-Die-allermeisten-Ueberwachten-sind-keine-Zielpersonen-2250440.html [Stand: 29.09.2014].

2 Wikipedia: „NSA warrantless surveillance (2001-07)." URL: http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_%282001%E2%80%9307%29 [Stand: 29.09.2014].

3 Zeit online: „National Security Letters. Google veröffentlicht geheime FBI-Nutzerabfragen." URL: http://www.zeit.de/digital/datenschutz/2013-03/google-national-security-letters [Stand: 29.09.2014].

Es ist also an dieser Stelle nur vernünftig, anzunehmen, dass Netzwerkgeräte aus Ländern mit sehr einflussreichen Geheimdiensten (zumindest USA und China) mit Hintertüren versehen sind.

Das große Problem an Hintertüren ist: Jeder kann sie benutzen, auch ein potentieller Mitbewerber oder Kriminelle. So geschehen bei einer großen US-Kaufhauskette, die im Advent 2013 den Diebstahl von Kreditkartendaten zu beklagen hatte. Dabei wurden die Kreditkartenlesegeräte in allen Filialen des Unternehmens vermutlich über eine Backdoor mit einer Malware infiziert, die es den Angreifern ermöglichte, Namen, Kartennummer, Ablaufdatum und Sicherheitscode der Karten auszulesen[4].

Aber auch in Deutschland kommen solche Hackerangriffe vor: Die Router eines großen deutschen Telekommunikationsanbieters konnten ausgespäht und so manipuliert werden, dass sie ohne Wissen des Kunden ein von den Hackern vorgegebenes Ziel mit Anrufen terrorisieren. Besonders pikant war dabei die Tatsache, dass der Telekommunikationsanbieter schon mehr als ein halbes Jahr über eine entsprechende Sicherheitslücke informiert war[5].

Werden Hintertüren nicht ab Werk eingebaut, behelfen sich Geheimdienste anders: Sie fangen die Geräte ab, bauen Späh-Software ein und verschicken die Ware dann weiter an die entsprechenden Kunden[6]. Außerdem beschäftigen sie sich auch mit diversen Verschlüsselungsstandards und schwächen diese absichtlich[7]. So wird vermutet, dass das weit verbreitete Protokoll IPSec deswegen so schlecht dokumentiert und kompliziert ist, damit es von Geheimdiensten ausspioniert werden konnte[8]. Belegt ist aber, dass etwa US-amerikanische Hersteller von Verschlüsselungslösungen Geräte für den Regierungsgebrauch gegen Bezahlung durch die NSA mit absichtlich gebrochener Verschlüsselung verkauft haben[9].

---

4 Jörg Breithut: „Hackerangriff: US-Kaufhauskette Target bestätigt millionenfachen Datendiebstahl." In: Spiegel Online. URL: http://www.spiegel.de/netzwelt/web/hacker-angriff-auf-us-kaufhauskette-target-a-940301.html [Stand 29.09.2914].

5 Konrad Lischka: „Sicherheitslücke: Kriminelle kapern Vodafone-Router." In: Spiegel Online. URL: http://www.spiegel.de/netzwelt/web/vodafone-easybox-kriminelle-nutzen-sicherheitsluecke-aus-a-917819.html [Stand 29.09.2014].

6 Focus online: „Cisco-Chef protestiert bei Obama. NSA öffnet heimlich Pakete – und installiert Späh-Software." URL: http://www.focus.de/finanzen/news/unternehmen/cisco-chef-protestiert-bei-obama-nsa-oeffnet-heimlich-pakete-und-installiert-spaeh-wanzen_id_3861181.html [Stand: 29.09.2014].

7 heise online: „NSA und GCHQ: Großangriff auf Verschlüsselung im Internet." URL: http://www.heise.de/security/meldung/NSA-und-GCHQ-Grossangriff-auf-Verschluesselung-im-Internet-1950935.html [Stand: 29.09.2014].

8 Andy Greenberg: „Ten Things We've Learned About The NSA From A Summer Of Snowden Leaks." In: Forbes. URL: http://www.forbes.com/sites/andygreenberg/2013/09/09/ten-things-weve-learned-about-the-nsa-from-a-summer-of-snowden-leaks/ [Stand: 29.09.2014].

9 Jörg Thoma: „Bsafe. NSA bezahlte RSA Security, um Krypto-Backdoor einzusetzen." In: golem.de. URL: http://www.golem.de/news/bsafe-nsa-zahlte-rsa-security-um-krypto-backdoor-einzusetzen-1312-103540.html [Stand: 29.09.2014].

All diese Vorkommnisse zeigen, dass allgemein ein Umdenken stattfinden muss. Unternehmen sollten nicht länger auf die Sicherheit namhafter Hersteller vertrauen, nur weil ihnen der Name bekannt ist; genauso wenig sollten sie darauf setzen, dass ihr jeweiliger Internetanbieter die übertragenen Daten gesetzeskonform behandelt. Weltweit setzen Geheimdienste auf massenhafte Datenüberwachung und treffen Vorkehrungen, um massenhaft Daten zu überwachen – egal, ob mit oder ohne freiwillige Kooperation bekannter Routerhersteller und großer Internetanbieter. Die eigentliche Krux an der Sache ist jedoch: Die beschriebenen Sicherheitslücken in Geräten und Verschlüsselungssoftware können sich auch andere Angreifer zunutze machen, zum Beispiel ein Wettbewerber, der sich einen Vorteil verschaffen möchte und aus diesem Grunde die Geschäftsgeheimnisse anderer ausspioniert. Anders gesagt: Der NSA-Skandal hat insgesamt viel weitreichendere Folgen, als gemeinhin angenommen und betrifft nicht nur große Unternehmen, die aufgrund ihrer vielen Beschäftigten in den Fokus von Geheimdiensten rücken können, sondern auch kleine Firmen, deren wirtschaftlicher Erfolg noch viel mehr von der Wahrung ihrer Geschäftsgeheimnisse abhängt.

GRUNDREGELN DER NETZWERKSICHERHEIT

Netzwerksicherheit ist ein extrem komplexes Thema und umfasst Netzwerk-interne und -externe Faktoren. Die folgenden Ratschläge sind Anbieter- und Hersteller-unabhängig und bieten dadurch ein gewisses Grundgerüst dafür, wie Sie ein sicheres Datennetzwerk aufsetzen müssen, damit Ihre Unternehmensgeheimnisse gewahrt bleiben.

1. Nutzen Sie möglichst viele verschiedene Verschlüsselungsarten

Verschlüsselungstechnologien gibt es viele und nur sehr wenige davon gelten gemeinhin als relativ sicher. Daher sollten Sie eine Netzwerklösung wählen, die auf verschiedene Verschlüsselungstechniken an verschiedenen Stellen der Infrastruktur baut. Am sichersten ist eine Kombination von Software- und Hardware-basierten Verschlüsselungsmechanismen, denn so muss ein potentieller Angreifer mindestens zwei Attacken gleichzeitig ausführen, um an die begehrten Daten zu kommen: Er muss die jeweiligen Netzwerkgeräte selbst manipulieren und parallel den Programmcode verändern.

2. Übertragen Sie Ihre Daten über möglichst viele Netzwerke

Das klingt zunächst paradox, aber je mehr Providernetze Sie nutzen können, desto sicherer wird Ihre Datenkommunikation. Voraussetzung ist hierfür, dass Sie verschiedene Internetverbindungen von verschiedenen Anbietern und über verschiedene Übertragungsmedien gebündelt nutzen können.

Im Idealfall verschlüsselt und „zerhackt" Ihre Anbindungslösung Ihren Datenstrom so, dass die einzelnen Datenfragmente über mehrere unterschiedliche WAN-Verbindungen verschiedener Anbie-

ter verteilt übertragen werden können, denn dadurch wird es ein potentieller Angreifer sehr, sehr schwer haben, Ihre Daten abzufangen. Er wäre dann gezwungen, zuerst herauszufinden, wie viele Verbindungen Sie überhaupt nutzen und über welche Medien Sie diese herstellen. Danach müsste er die verschiedenen Datenfragmente abfangen und herausfinden, welches Datenfragment zu welchem Datenstrom gehört. Das kann er aber nur, wenn er zunächst in allen Netzwerken die jeweils unterschiedlichen Verschlüsselungen überwindet. Dazu wäre eine Komplettaufzeichnung sämtlichen Datenverkehrs aller Providernetzwerke notwendigen, was schwer zu bewerkstelligen ist.

3. Kaufen Sie nach länderspezifischem Recht anstatt Markennamen

Geheimdienste gibt es in jedem Land, das eine gewisse wirtschaftliche Bedeutung hat. Das ist ungeschriebenes Gesetz und an sich durchaus sinnvoll. Bei der Wahl der richtigen Datensicherheitslösung ist es jedoch wichtig, darauf zu achten, welche Rechte Geheimdienste in dem Land haben, wo der Hersteller und/oder Anbieter Ihrer Netzwerkkomponenten sitzt.

Achten Sie bei Herstellern auch auf deren Produktionskette. Von der Entwicklung von Hardware und Software bis hin zur Produktion und Qualitätssicherung eines Geräts sollten alle Prozesse an einem Standort geschehen, vorzugsweise in einem Land wie Deutschland, das die Wahrung von Bürgerrechten bislang sehr genau nimmt. Nur so hat ein Hersteller auch ausreichend Kontrolle über seine Produktionskette und minimiert dadurch die Möglichkeiten, dass seine Produkte gegebenenfalls sogar ohne sein Wissen kompromittiert werden.

Im Gegensatz dazu gibt es, wie bereits beschrieben, in den USA und China Geheimgerichte, die den Einbau von Hintertüren und Späh-Software in Router und andere Netzwerkprodukte anordnen dürfen, oft kombiniert mit einer lebenslangen Schweigepflicht. Das bedeutet, bei Produkten vieler namhafter Hersteller aus den USA und China ist Vorsicht geboten, was sichere Datenkommunikation betrifft.

4. Gönnen Sie sich den Luxus einer gewissen Paranoia

Vor Edward Snowden galten Vermutungen darüber, dass Geheimdienste massenhaft Datenverkehr im Internet abfangen und dadurch Bürgerrechte aushebeln, als Fantasien von Verschwörungstheoretikern. Es hat sich leider herausgestellt, dass diese Vermutungen nur allzu wahr waren. Überlegen Sie, wie viel Ihnen Ihre Unternehmensgeheimnisse wert sind, und leisten Sie sich Skepsis. Setzen Sie lieber mehr Systeme zum Schutz Ihrer Daten ein als zu wenige – zu viel Datensicherheit gibt es nicht.

5. Fordern Sie Garantien

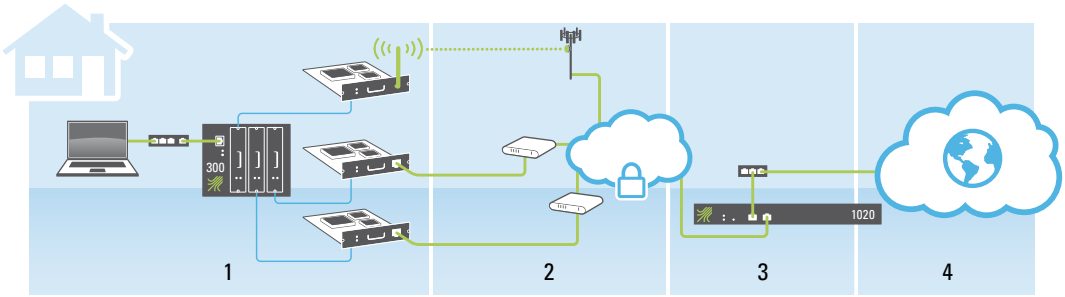
Wie eingangs festgestellt, reicht es schon lange nicht mehr, nur Vertrauen in eine Marke zu haben: Namhafte Internetanbieter und Hersteller von Netzwerkprodukten bieten nicht automatisch ausreichend Datensicherheit, nur weil ihr Name bekannt ist. Vielmehr sind sie heutzutage in der Pflicht, zu beweisen, dass sie nicht mit Geheimdiensten zusammenarbeiten.

Lassen Sie sich also von Ihrem Anbieter oder Hersteller eine verbindliche Garantie ausstellen, dass er keine Hintertüren in seine Geräte einbaut, keine Späh-Software verwendet, keine Verschlüsselungen umgeht und auch sonst in keinster Weise mit Geheimdiensten kooperiert. Sieht sich Ihr Anbieter oder Hersteller dazu nicht in der Lage, sollten Sie im Hinblick auf die Sicherheit Ihrer Geschäftsgeheimnisse einen Wechsel auf eine andere Anbindungslösung in Betracht ziehen.

LÖSUNGSANSATZ

Höchstmögliche Datensicherheit erreichen Sie nur durch eine in sich geschlossene und von Anfang an durchdachte Anbindungsinfrastruktur. Eine solche bietet Ihnen Viprinet mithilfe der bewährten und vor allem hochsicheren echten WAN-Bündelung.

Viprinet ist ein Zwei-Komponenten-System bestehend aus einem Multichannel VPN Router und einem Multichannel VPN Hub. Der Datenstrom vom LAN wird vom Multichannel VPN Router zerteilt, verschlüsselt und auf die Internetanschlüsse (hier: 2x DSL, 1x LTE) aufgeteilt (1). Die verschlüsselten Daten passieren aufgeteilt die Netze der verwendeten ISPs (2) und erreichen den Multichannel VPN Hub im Rechenzentrum (3). Dieser Hub übermittelt die Datenfragmente entweder direkt an einen Viprinet-Router in einer anderen Niederlassung, welcher die Fragmente wieder entschlüsselt und korrekt zusammensetzt; oder der Hub entschlüsselt die Datenfragmente selbst und formt sie wieder zu einem Datenstrom, den er anschließend zum eigentlichen Ziel im Internet weiterleitet (4). Ebenso wird in der Gegenrichtung verfahren.



Damit wird Ihr Datenstrom gemäß Grundregel Nr. 2 („Übertragen Sie Ihre Daten über so viele Anbieternetzwerke wie möglich") in kleinere Fragmente zerteilt, die so viele Übertragungsmedien und Anbieternetzwerke wie möglich passieren. Für sich genommen sind diese Datenfragmente nutzlos: Nur Viprinet-Geräte sind in der Lage, sie wieder korrekt zu einem von anderen Anwendungen nutzbaren Datenstrom zusammen zu fügen. Zudem werden der Datenstrom noch vor der Zerteilung gemäß Grundregel Nr. 1 („Setzen Sie auf möglichst viele verschiedene Verschlüsselungsarten") mithilfe verschiedener Methoden verschlüsselt. Die in Viprinet-Routern und -Hubs verwendeten Verschlüsselungen bestehen immer aus einer Mischung von Hardware- und Softwarelösungen (AES 256 Bit CBC, 2048-bit RSA-Schlüssel mit SHA256-Zertifikaten, TLS 1.2, Diffie-Hellman-Schlüsselaustausch mit elliptischen Kurven u.a.), die von neutralen Lieferanten bezogen und mit Eigenentwicklungen kombiniert werden. Damit ist Viprinet-Technologie Made in Germany – passend zu Grundregel Nr. 3 („Wählen Sie Ihre Netzwerklösung nach länderspezifischem Recht, nicht nach Marken").

Natürlich bleibt auch bei Viprinet – genauso wie bei jedem anderen Hersteller von Netzwerkkomponenten – ein physikalischer Angriff auf die verwendeten Geräte immer ein Risiko. Um diesen bestmöglich vorzubeugen, sollten Viprinet-Hubs prinzipiell in sicherheitszertifizierten Rechenzentren installiert und das entsprechende Rack gegen unbemerktes Eindringen abgesichert werden. Auch bei Viprinet-Routern an den einzelnen Standorten sollte ein physikalischer Zugriffsschutz, zum Beispiel durch einen abschließbaren Raum, gewährleistet sein – entsprechend Grundregel Nr. 4 („Gönnen Sie sich den Luxus einer gewissen Paranoia").

Zu guter Letzt garantiert der Geschäftsführer von Viprinet, Simon Kissel, persönlich, dass in Viprinet-Geräten keine Hintertüren eingebaut werden. Viprinet verwendet keine Späh-Software, umgeht keine Verschlüsselungen und kooperiert auch sonst in keinster Weise mit Geheimdiensten – bislang nicht und auch nicht in Zukunft. So unterstützt Viprinet Sie auch beim Befolgen von Grundregel Nr. 5 („Fordern Sie Garantien").

FAZIT

Um Unternehmensnetzwerke und damit letztendlich auch Geschäftsideen ausreichend gegen Hackerangriffe, Industriespionage und das Abhören durch Geheimdienste zu schützen, braucht es einen gewissen technischen Aufwand, aber auch Offenheit neuen Ideen gegenüber. Die Befolgung einiger weniger Regeln ermöglicht Unternehmen die Auswahl einer ausreichend sicheren Netzwerklösung und damit die Wahrung ihrer Geschäftsinteressen. Der NSA-Skandal hat gezeigt, wie kreativ Geheimdienste sind, wenn es um die Auslegung von Bürgerrechten geht – seien Sie als Unternehmer also kreativer, wenn es darum geht, Ihre Rechte zu wahren.