SECURITY OF CORPORATE NETWORKS IN THE ERA OF DATA SURVEILLANCE

EXECUTIVE SUMMARY

The revelations by Edward Snowden showed to which extent and with which self-conception intelligence services monitor any Internet traffic and thus illegally turn respected citizens into suspects. It's the first time that the security of company data has been brought to the center of interest across all branches. While data security was a nice extra and was often unattended, more and more companies now look at it as an essential part of their connectivity solution. However, it shall be advised not to pick a "whatever comes first" offer for data security, as in too many cases these offers are made by intelligence services that were meant to be locked out in the first place.

This whitepaper addresses all persons who are in charge of data security on behalf of an enterprise. It furnishes background knowledge how intelligence services get unnoticed access to practically all digital data and it explains what to pay attention to if you wish to protect your data. Also, it lists security solutions that are already available.

INTRODUCTION

In order to reach such an extent of data monitoring as described by Edward Snowden – 160,000 intercepted emails, hundreds of pages long chat-transcripts, and cataloging everyday life of more than 10,000 people in the USA alone[1] – it takes a sophisticated system that consists of two steps: to get access without being noticed, and to lever out encryption mechanisms.

DATA KRAKEN AT YOUR BACK DOOR

When looking for unnoticed access to confidential data, it's best to use installed entries, so-called "back doors". That's why the US-American FISA Court ("Foreign Intelligence Surveillance Act") constantly approves monitoring requests from the NSA even though its task is to verify the underlying necessity with utmost scrutiny[2]. By sending out National Security Letters – 'orders' issued by a body which lacks judicial authority – the FBI may demand from telephone and network providers to disclose their data; in many cases, providers are then even denied to inform their clients about such an incident[3]. Hence, it is reasonable to assume that network devices from countries with

[1] Gellman, B., Tate, J. and Soltani, A.: "In NSA-intercepted data, those not targeted far outnumber the foreigners who are." In: The Washington Post. URL: http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?tid=pm_pop [by 9/29/2014].

[2] Wikipedia: "NSA warrantless surveillance (2001-07)." URL: http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_%282001%E2%80%9307%29 [by 9/29/2014].

[3] Greenberg, A.: "Google Breaks Silence On FBI's National Security Letters The Demand Its Users' Data." In: Forbes. URL: http://www.forbes.com/sites/andygreenberg/2013/03/05/google-breaks-silence-on-fbis-national-security-letters-that-demand-its-users-data/ [by 9/29/2014].

influential intelligence services (at least the USA and China) are fitted with installed back doors. The big problem with back doors is that everybody can use them, even a potential competitor. This happened to a large US retail chain when in December 2013, the company had to deal with credit theft. In this incident, malware was installed on the chain's point-of-sale (POS) devices that enabled the attackers to intercept customers' names, card numbers, expiry dates, and security codes[4].

Hacker attacks like these also happen in Europe. The routers of a large German telecommunications provider were spied upon and manipulated in a way that they would terrorize a target specified by the attackers with countless telephone calls. Here, it was particularly revealing that the provider had been informed about the respective security leak more than half a year earlier[5].

If back doors are not installed ex works, intelligence services chose another option: They get hold of the appliances, install the spyware and send the merchandise on to the respective customer[6]. In addition, intelligence services deal with various encryption standards with the aim to weaken these intentionally[7]. It is assumed that the widely spread IPSec protocol has been documented in such poorly fashion and is so complicated in order to be spied out by intelligence services[8]. It has been documented already that, for instance, US-American manufacturers of encryption solutions have sold appliances designated for government use with intentionally broken encryption against payment by the NSA[9].

All these incidents demonstrate that a general rethinking has to take place. Entrepreneurs should no longer rely on the security of well-known manufacturers simply because they know their names; much less should they trust that their current Internet provider deals with the transmitted data as prescribed by law. Intelligence services worldwide choose to monitor data on a huge scale and they take any precautions to monitor data – irrespective of whether well-known router manufacturers and Internet providers are willing to cooperate deliberately or not. The problem with that is that security holes in appliances and encryption software may also be used by other attackers, e.g. a competitor who wishes to take an advantage therefrom and who, as a consequence, spies out the trade secrets of third parties. In other words: The consequences evolving from the NSA

[4] Perlroth, N.: "Target Struck in the Cat-and-Mouse Game of Credit Theft." In: The New York Times. URL: http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html?_r [by 9/29/2014]

[5] Parker, M.: „Vodafone EasyBox router hacked by criminals for making anonymous VOIP calls." In: Mashabler. URL: http://www.mashabler.com/2013/08/vodafone-easybox-router-hacked-by.html [by 9/29/2014].

[6] Hesseldahl, A.: "In Letter to Obama, Cisco CEO Complains About NSA Allegations." In: Re/code. URL: http://recode.net/2014/05/18/in-letter-to-obama-cisco-ceo-complains-about-nsa-allegations/ [by 9/29/2014].

[7] Ball, J., Borger, J. and Greenwald, G.: "Revealed: how US and UK spy agencies defeat internet privacy and security." In: theguardian. URL: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [by 9/29/2014].

[8] Greenberg, A.: „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/ [by 9/29/2014].

[9] Menn, J.: „Exclusive: Secret contract tied NSA and security industry pioneer." In: Reuters. URL: http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 [by 9/29/2014].

scandal will all in all have a much further reach than is generally expected. They will not only have an impact on huge corporations who might become the center of attention of intelligence services for the sheer number of their employees, but also on small enterprises whose economic success depends on the confidentiality of their trade secrets to a much larger extent.

BASIC RULES FOR NETWORK SECURITY

Network security is an extremely complex subject and comprises network-internal and -external factors. The following advice is independent from providers and manufacturers, and may thus offer you some basic knowledge how to set-up a secure data network to protect your company's trade secrets.

1. Use as many different encryption methods as possible

There are many encryption technologies in place and only a few of them may be deemed to be relatively secure. You should therefore choose a network solution that uses several encryption technologies on different places of the infrastructure. The highest level of security is provided by a combination of software- and hardware-based encryption mechanisms as this would force an attacker to launch at least two attacks simultaneously in order to get hold of the much sought-after data: The attacker would have to manipulate the respective network appliances, and change the program code at the same time.

2. Transmit your data via as many providers' networks as possible

This may sound a bit paradox but the more provider networks you can use, the higher the level of security of your data communication will be. However, a prerequisite is that you're able to use several Internet connections from different providers across different transmission media and that these connections are bonded together.

Ideally, your connectivity solution encrypts and "chops up" your data stream in a way that the single data fragments will be transmitted via several different WAN connections of different providers. This would make it very difficult for potential attackers to intercept your data because they would then be forced to find out how many connections you use and via which media these would be established. Thereafter, they would have to intercept all the different data fragments and figure out which data fragment belongs to which data stream. However, they would only be able to do so after breaking all encryptions used by Viprinet – every single one of them created specifically for each provider network involved. For that, potential attackers would need to completely record all data traffic of all provider networks which is quite elusive.

3. Buy according to country-specific law instead of brand names

Intelligence services can be found in every country that has gained a certain economic importance. It is an unwritten law and it definitely makes sense. However, when making your choice which data security solution to pick it is important to pay some attention to the rights entitled to the intelligence services of the country in which the manufacturer and/or supplier of your network components have their legal seats.

Please also pay attention to the manufacturer's production chain. From the development of the hard- and software to the production and quality assurance of an appliance, all production processes should be made at a single location; preferably in a country like Germany where civil rights are protected quite accurately to date. Only by that, manufacturers are able to exercise sufficient control over their production chains and minimize the risk of their products being compromised without their noticing.

To the contrary, there are secret courts in the USA and in China that may order the installation of back doors and spyware into routers and other network products; in many times combined with a lifelong non-disclosure obligation. This means that as far as many products from the USA and China are concerned, it would be wise to pay attention with respect to data communication.

4. Grant Yourself some Data Security Paranoia

In the era before Edward Snowden, assumptions that intelligence services might intercept data traffic on the Internet on a huge scale, and by doing so might circumvent civil rights were qualified as phantasies from conspiracy theorists. These assumptions did, however, prove to be true. Make up your mind on how much your enterprise's trade secrets would be worth in your eyes and raise some doubt. Better to use more systems for protecting your data than too little -- there is no such thing as too much data security.

5. Demand Guarantees

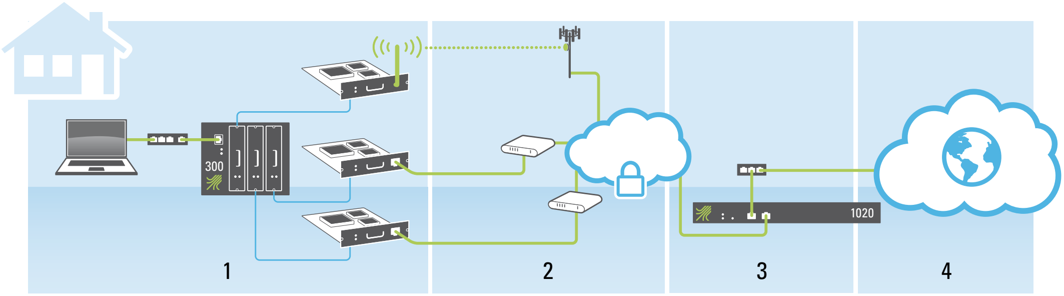
As already determined at the beginning of this whitepaper, it doesn't suffice any more to have faith in a trademark: Well-known Internet providers and manufacturers of network products don't automatically offer sufficient data security simply because their names are known. Today, they are in fact under an obligation to prove that they do not collaborate with intelligence services.

Please ask your provider or manufacturer to issue a legally-binding warranty that he does not install any back doors into his appliances, use any spyware, circumvent any encryptions nor cooperate with intelligence services in any way whatsoever. If your provider or manufacturer is unwilling or unable to comply with your request, you might consider choosing another connectivity solution to keep your trade secrets protected.

KEY TO THE SOLUTION

You should be aware that you will only obtain the maximum data security in an integrated connectivity infrastructure that has already been well planned from the beginning. One and maybe the best example for such an infrastructure is the well-proven and first and foremost highly secure real WAN bonding of Viprinet.

Viprinet is a two-component system based on a Multichannel VPN Router and a Multichannel VPN Hub. The data stream from the LAN is fragmented by the Multichannel VPN Router, encrypted, and distributed (1) onto all available Internet connections (here: 2x DSL, 1x 4G). The encrypted and fragmented data passes the networks of the utilized ISPs (2) and reaches the Multichannel VPN Hub in the data center (3). This hub then transmits the data fragments either directly to a Viprinet router at another site which in turn decrypts the data stream and reassembles it correctly; or the hub decrypts the data fragments itself and restores the data stream before forwarding it to its actual destination on the Internet (4). The same goes for the opposite direction.



By that, your data stream is separated into smaller fragments that pass through as many transfer media and provider networks as possible, compliant with basic rule no. 2 (“Transmit your data via as many providers’ networks as possible”). The data fragments by themselves are useless: Only Viprinet devices are able to correctly reassemble them to a data stream that can be utilized by other applications. In addition, the data stream encrypted using diverse methods before the fragmentation, compliant with basic rule no. 1 (“Use as many different encryption methods as possible”). The encryptions generated by Viprinet routers and hubs Viprinet encryption always consist of a mixture of hardware and software solutions (e.g. AES 256 Bit CBC, 2048-bit RSA key with SHA256 certificates, TLS 1.2, or Diffie-Hellman key exchange with elliptic curves) that are purchased from neutral suppliers and combined with proprietary development. This is why Viprinet technology is “Made in Germany”, compliant with basic rule no. 3 (“Choose your network solution according to the laws of the specific country, not according to trademarks”).

At this point, it has to be made clear that a physical attack on the devices used will always stay a risk, even with Viprinet technology. In order to prevent such attacks in the best possible way, Viprinet hubs should only be installed in data centers that are specially certified for their security, and the respective rack should also be protected against unnoticed intrusion. In addition, physical protection against unauthorized access should be ensured for Viprinet routers at the respective sites, e.g. by installing them in a lockable room – according to basic rule no. 4 ("Grant Yourself some Data Security Paranoia").

Last but not least, Viprinet CEO Simon Kissel personally guaranteed that Viprinet devices are free of any back doors. Viprinet neither uses spy software nor circumvents any encryptions. Also, Viprinet has never cooperated with intelligence services in any way whatsoever nor will ever do so. This is how Viprinet assists you in obeying basic rule no. 5 ("Demand Guarantees").

CONCLUSION

In order to protect corporate networks and, ultimately, business ideas sufficiently against hacker attacks, industrial espionage, and the interception from intelligence services, entrepreneurs need to invest a certain technical effort and they need to be open to new ideas. Obeying a few rules allows companies to select a sufficiently secure network solution, thus protecting their business. The NSA scandal has shown how creative intelligence services are when it comes to interpreting civil rights – now it's your turn as an entrepreneur to make sure to be even more creative when it comes to protecting your rights.