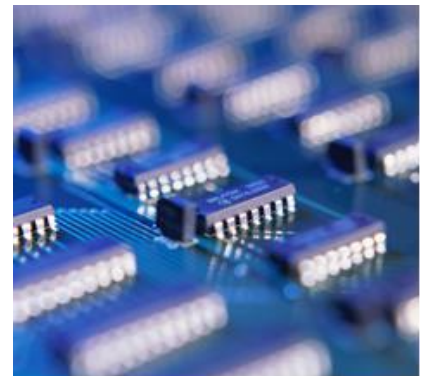


IT security: Convergence of endpoint and network security?

Dear Reader,

As you might have read in the newspapers, in the last couple of weeks one of the most significant security flaws in recent years was revealed: An error in a type of internet encryption security, known as OpenSSL, was disclosed. This standard is one of the most widely used security methods across all industries¹. As a result, the so-called “Heartbleed” bug was able to expose millions of passwords, credit card numbers and other pieces of sensitive information. Two-thirds of the worlds’ web-sites were affected and this vulnerability has been undetected for two years². Although a patch has been issued, all users are encouraged to update their passwords on sensitive websites.



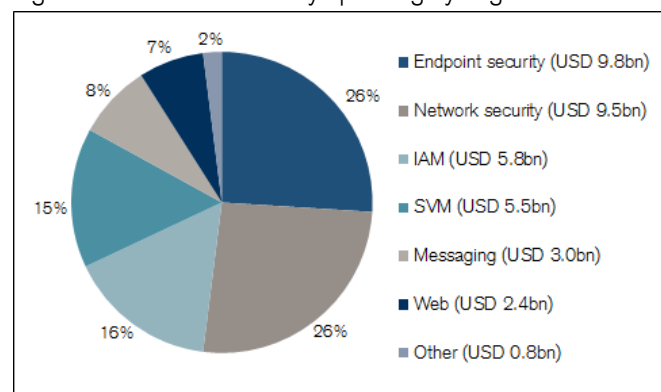
As such high profile incidents have shown, hackers are gaining access to supposedly secure IT networks through unlikely places such as printers, thermostats and videoconferencing equipment. Therefore we believe a 100% secure IT network is nearly impossible to guarantee. An integrated security approach is needed which combines endpoint security (e.g. anti-virus) and network security (e.g. authorization of data access in a network). In this paper we describe in a first step the IT security market. Secondly, we provide an overview of the current threat landscape and its challenges. To conclude, we highlight a technological trend as a possible solution.

The market for IT security

The recent IT security incidents as well as the proliferation of mobile devices, cloud computing and available connectivity have created a significant need for modern security solutions. An emerging theme is in our opinion the convergence of endpoint security and network security.

To get a better understanding of the environment, fig. 1 shows the worldwide security spending by segment. According to IDC, annual spending for IT security, endpoint security and network security combined represent over 50% of the total

Fig. 1: Worldwide IT security spending by segment



Source: IDC, Barclays, Credit Suisse

¹ OpenSSL is an open-source software used to secure the traffic flow between servers and the users’ computers. Websites, network-equipment companies and governments use these tools to protect personal and other sensitive information online. The Secure Sockets Layer (SSL) denotes an encryption protocol, which is indicated by a closed padlock appearing on browsers next to a website’s address (source: The Wall Street Journal (2014): Internet Security Relies on Very Few, in: The Wall Street Journal, April 11th 2014, URL: <http://online.wsj.com/news/articles/SB20001424052702303873604579495362672447986>, April 22nd 2014).

² Source: Financial Times (2014): Companies rush to protect against cyber security flaw, in: The Financial Times, April 12th 2014, p. 9.

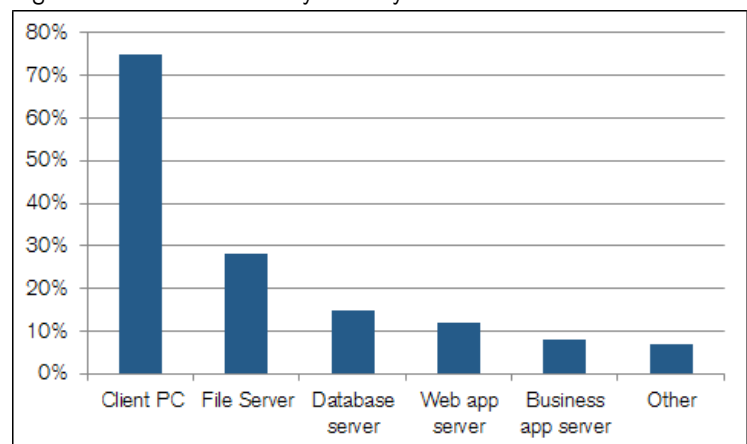
product related spending (USD 9.8bn and USD 9.5bn respectively). Additionally, adjacent markets include in this context identity and access management (IAM, USD 5.8bn), security and vulnerability management (SVM, USD 5.5bn), messaging (USD 3.0bn), web (USD 2.4bn) and others (USD 0.8bn).

The current threat landscape in IT security

The modern threat landscape has evolved substantially over the last couple of years, shifting from unwanted ads or even denial of service attacks to much more sophisticated and targeted attacks. According to the Swiss Reporting and Analysis Centre for Information Assurance, the efficiency of anti-virus products is restricted in particular to common, widespread malware. In case of targeted attacks which only affects a fraction of the users, an efficient detection is practically impossible³. On the other hand, the technological opportunities in increasing the operational efficiency the internet is offering has flooded the corporate networks with personal and confidential data. As a consequence, vulnerabilities are rising as more and more third party firms have been granted remote access to corporate systems. This trend is giving sophisticated cyber criminals possibilities to exploit data for profit. Today's common threats that security solutions need to address are as follow:

- Advanced persistent threats (APT): APT are a set of stealthy and continuous computer hacking processes, often orchestrated by humans targeting a specific entity. APT usually targets organizations or nations for business or political motives. APT processes require a high degree of covertness over a long period of time⁴.
- Zero-day exploits: A Zero-day exploit is a piece of software, data or a sequence of commands that takes advantage of a vulnerability in order to cause unintended or unanticipated behaviour on computers. Some hackers do not publish their exploits and keep them private. Because these vulnerabilities have not been discovered, they are particularly dangerous⁵.
- Polymorphic codes: A polymorphic code is a code that mutates while keeping the original algorithm intact to evade detection. It can occur in a number of ways through filename changes or encryption⁶.
- Blended threats: A blended threat combines multiple types of malware and uses multiple attack vectors to increase the severity of damage⁷.

Fig. 2: IT assets affected by security violations



Source: IDC, Barclays, Credit Suisse

In the past, traditional security solutions have struggled to adapt to these newer kind of threats because they are able to bypass traditional firewalls, intrusion detection and prevention tools, anti-virus and web-gateways. A survey conducted by IDC shows that the client PC is in more than 70%

³ Source: Reporting and Analysis Centre for Information Assurance MELANI (2014): Information Assurance: Situation in Switzerland and internationally, semi-annual report 2013/II (July – December), p. 30.

⁴ Source: Symantec (2014): What We Talk About When We Talk About APT, URL: <http://www.symantec.com/connect/blogs/what-we-talk-about-when-we-talk-about-apt>, 23.4.2014.

⁵ Source: Whitman (2012): Principles of Information Security: The Need for Security, 4th Edition, Boston, p. 53.

⁶ Source: URL: <http://searchsecurity.techtarget.com/definition/metamorphic-and-polymorphic-malware>, 23.4.2014.

⁷ Source: URL: <http://searchsecurity.techtarget.com/definition/blended-threat>, 23.4.2014.

of all cases the most affected IT equipment (fig. 2). In our opinion this is not surprising but it also highlights the need for better endpoint protection. Additionally the rise of tablets and smartphones as well as the trend in BYOD (“bring your own device”) have led to nightmares for IT administrators because of complications in the IT infrastructure. In our opinion, as more devices are connected to the corporate network, IT departments can no longer approach IT security from a network-only perspective. Therefore a convergence of endpoint and network security is needed. As a result network security policies need to include all physical endpoints.

To conclude

There is an ongoing debate among experts about which security layer (endpoint vs. network) is more critical to protect a corporation. We believe that both, network as well as endpoint solutions are equally important. In the past these two subsegments have traditionally operated independent of each other, but recently there has been increased interest in the prospect of a tighter integration between network and endpoint security⁸. We think the coupling of the two segments is very compelling, especially under the aspects of the advancements in cloud computing, big data analytics and threat intelligence. The use of virtualization, sandboxing and other containment techniques for security purposes has gained widespread adoption in the last couple of years. While these solutions have substantially improved the industry’s overall preparedness against modern cyber threats, each technique has some shortfalls, either security or performance related. Additionally like most emerging security trends, unfriendly actors have been fairly quick to adapt and bypass most containment solutions.

The revelation of the discussed Heartbleed incident will trigger more discussions about how to deal with IT security risks. It might reinforce the impression that the cyberspace can’t be trusted anymore⁹. Therefore a fair question is which other measures are required to increase the level of security. One aspect is comprehensibility: Should malware have found its way into a corporate network, it is important to understand by which way it entered. This is the only way to eliminate it completely from the network. As past incidents have shown, it can take several months or even years between intrusion of a malware into a network and its detection¹⁰. And finally the best prevention against such kind of incidents are well educated employees. Therefore regular employee training and awareness-raising are crucial.

For long-term oriented investors we believe the IT security theme is still early in its secular growth cycle. We do not think these kind of incidents will decline any time soon. Therefore we believe this segment can be an interesting long term investment opportunity. As a consequence, we are shareholders of leading companies in this attractive field.

Service

If you have any questions please do not hesitate to contact me by phone +41 (0)44 344 69 90 or e-mail: Dr. Patrick Kolb: patrick.kolb@credit-suisse.com

⁸ Especially after the recent acquisitions of Mandiant by FireEye and Cyvera by Palo Alto Networks.

⁹ Interestingly, according to the Financial Times AIG is offering an insurance policy to compensate companies for cyber-attacks that damage property and even harm people. The market for cyber insurance has been slow to develop because of lack of historical data to model the potential losses arising from cyber-attacks (source: The Financial Times (2014): AIG offers cyber policy add-on as threat to people and property rises, in: The Financial Times, April 24th 2014, p. 11).

¹⁰ Source: Verizon (2012): Verizon Data Breach Investigation Report 2012, fig. 40, p. 49.

Neither this document nor any copy thereof may be sent, taken into or distributed in the United States

This material has been prepared by the Private Banking & Wealth Management division of Credit Suisse ("Credit Suisse") and not by Credit Suisse's Research Department. It is not investment research or a research recommendation for regulatory purposes as it does not constitute substantive research or analysis. This material is provided for informational and illustrative purposes and is intended for your use only. It does not constitute an invitation or an offer to the public to subscribe for or purchase any of the products or services mentioned. The information contained in this document has been provided as a general market commentary only and does not constitute any form of regulated financial advice, legal, tax or other regulated financial service. It does not take into account the financial objectives, situation or needs of any persons, which are necessary considerations before making any investment decision. The information provided is not intended to provide a sufficient basis on which to make an investment decision and is not a personal recommendation or investment advice. It is intended only to provide observations and views of the said individual Asset Management personnel at the date of writing, regardless of the date on which the reader may receive or access the information. Observations and views of the individual Asset Management personnel may be different from, or inconsistent with, the observations and views of Credit Suisse analysts or other Credit Suisse Asset Management personnel, or the proprietary positions of Credit Suisse, and may change at any time without notice and with no obligation to update. To the extent that these materials contain statements about future performance, such statements are forward looking and subject to a number of risks and uncertainties. Information and opinions presented in this material have been obtained or derived from sources which in the opinion of Credit Suisse are reliable, but Credit Suisse makes no representation as to their accuracy or completeness. Credit Suisse accepts no liability for loss arising from the use of this material. Unless indicated to the contrary, all figures are unaudited. All valuations mentioned herein are subject to Credit Suisse valuation policies and procedures. It should be noted that historical returns and financial market scenarios are no guaranty of future performance.

Every investment involves risk and in volatile or uncertain market conditions, significant fluctuations in the value or return on that investment may occur. Investments in foreign securities or currencies involve additional risk as the foreign security or currency might lose value against the investor's reference currency. Alternative investments products and investment strategies (e.g. Hedge Funds or Private Equity) may be complex and may carry a higher degree of risk. Such risks can arise from extensive use of short sales, derivatives and leverage. Furthermore, the minimum investment periods for such investments may be longer than traditional investment products. Alternative investment strategies (e.g. Hedge Funds) are intended only for investors who understand and accept the risks associated with investments in such products.

This material is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of, or is located in, any jurisdiction where such distribution, publication, availability or use would be contrary to applicable law or regulation, or which would subject Credit Suisse and/or its subsidiaries or affiliates to any registration or licensing requirement within such jurisdiction. Materials have been furnished to the recipient and should not be re-distributed without the express written consent of Credit Suisse.

When distributed or accessed from the EEA, this is distributed by Credit Suisse Asset Management Limited (authorised and regulated by the Financial Conduct Authority) or any other Credit Suisse entities. When distributed in or accessed from Switzerland, this is distributed by Credit Suisse AG and/or its affiliates. For further information, please contact your Relationship Manager. When distributed or accessed from Brazil, this is distributed by Banco de Investimentos Credit Suisse (Brasil) S.A. and/or its affiliates. When distributed or accessed from Australia, this document is issued in Australia by CREDIT SUISSE INVESTMENT SERVICES (AUSTRALIA) LIMITED ABN 26 144 592 183 AFSL 370450.

Copyright © 2014. CREDIT SUISSE GROUP AG and/or its affiliates. All rights reserved.

Liechtenstein: Investment products can be marketed from Switzerland vis-à-vis professional clients in existing client relationships.