

SECURITY THREATS AND TRENDS

JANUARY 2009

SECODE AB

Secode helps companies and organizations gain insight, competence and thereby control over their operations from a complete IT security perspective. We deliver proactive and perpetual vigilance within two areas: 24/7 Managed Security Services and Security Consulting.

The Company was originally founded in 1986 as System Sikkerhet A/S, in Arendal, Norway. In 2000, Secode AB was founded in Sweden and started its 24/7 Managed Security Services and Security Consulting. The two companies merged in January 2004, thereby forging the leading Digital Security Company in the Nordic region. In March 2006 the Finnish IT-security company Netsol OY (founded in 1996) was merged into Secode. From the first of January 2007 Secode has established sales-offices in both Denmark and The Netherlands and delivers IT-security services to customers in these countries as well. Secode helps many customers in private and public sectors, from seven different locations, using close to 85 security specialists. These specialists have long experience from building large computer networks and/or up-to-date IT security competence. Secode AB today has more than 100 employees.

All this together makes Secode the leading Northern European Digital Security Company within Managed Security Services combined with IT-Security Consultancy Services.

TABLE OF CONTENTS

INTRODUCTION	4
NEWS OF THE MONTH.....	5
FOCUS OF THE MONTH – HARDWARE ENCRYPTION.....	7

INTRODUCTION

This report is built on two main parts: News of the Month and Focus of the Month.

News of the Month is a chapter which presents the biggest IT security incidents registered by other media. This may be deep analysis, new viruses, new vulnerabilities, or other IT security news.

Focus of the Month is an article about relevant topics within IT Security. These might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

NEWS OF THE MONTH

During a month, several vulnerabilities will be published, and there will have been many security related news. This chapter presents the most important vulnerabilities and the most interesting news. Most cases, if not all, have been presented in Secode Norway's newsletter during this month.

PUBLISHED VULNERABILITIES

VLC Media Player Real Demuxer Integer Overflow Vulnerability
<http://www.videolan.org/security/sa0811.html>

VMSA-2008-0019 VMware Hosted products and patches for ESX and ESXi resolve a critical security issue and update bzip2
<http://lists.vmware.com/pipermail/security-announce/2008/000046.html>

Firefox 'plug-in' harvests web passwords
<http://www.bitdefender.co.uk/NW900-uk--BitDefender-detects-novel-approach-to-stealing-web-passwords.html>

Sun Java JDK / JRE Multiple Vulnerabilities
Link: <http://secunia.com/advisories/32991/>

Solaris vulnerabilities
Link: <http://securitytracker.com/alerts/2008/Dec/1021359.html>

Vulnerability in WordPad Text Converter Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/advisory/960906.mspx>

Citrix Application Gateway Management Interface SQL injection Issue
<http://support.citrix.com/article/CTX119315>

MediaWiki Multiple Vulnerabilities
<http://lists.wikimedia.org/pipermail/mediawiki-announce/2008-December/000080.html>

Firefox 3.0.5 fixes several security issues.
<http://www.mozilla-europe.org/no/firefox/>

Opera releases update for 'extremely severe' vulns
<http://www.opera.com/docs/changelogs/windows/963>

Sikkerhetsoppdatering for Internet Explorer (960714)
Link: <http://isc.sans.org/diary.html?storyid=5515>

Adobe Flash Player for Linux Remote Code Execution Vulnerability
<http://www.adobe.com/support/security/bulletins/apsb08-24.html>

Microsoft Security Advisory (961040) – SQL Server
<http://www.microsoft.com/technet/security/advisory/961040.mspx>

IN THE NEWS

A new issue of (IN)SECURE Magazine has been released
<http://www.net-security.org/dl/insecure/INSECURE-Mag-19.pdf>

Apple deletes Mac antivirus suggestion
http://news.cnet.com/8301-1009_3-10111958-83.html?tag=mncol:title

Beware of Fake Antivirus Products, According to BitDefender Labs' Top E-Threats in November

<http://news.bitdefender.com/NW903-en--Beware-of-Fake-Antivirus-Products-According-to-BitDefender-Labs%E2%80%99-Top-E-Threats-in-November.html>

Top 10 Coolest Hacking Moments in 2008

http://www.networkworld.com/community/node/36250?ts0hb&story=ts_purser

Google Chrome Receives Lowest Password Security Score

<http://www.info-svc.com/news/2008/12-12/>

Daft list names Firefox, Adobe and VMWare as top threats

http://www.theregister.co.uk/2008/12/12/app_threat_list/

Hackers Compromise Legit Web Sites to Target Microsoft IE Flaw

<http://www.eweek.com/c/a/Security/Hackers-Compromise-Legit-Web-Sites-to-Target-Microsoft-IE-Flaw/?kc=rss>

Europe's elite banks collaborate to combat cybercrime

<http://www.net-security.org/secworld.php?id=6854>

Hackers exploit IE bug with 'insidious' Word docs

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9123898&taxonomyId=17&intsrc=kc_top

Firefox 2.0.20 arrives with missed patch

<http://www.heise-online.co.uk/security/Firefox-2-0-20-arrives-with-missed-patch--/news/112297>

Small laptops pose a big security threat

<http://www.gss.co.uk/news/2008/12/?&id=5758>

FOCUS OF THE MONTH – HARDWARE ENCRYPTION

We read it in the news almost daily; data leakage and security breaches. Personal information belonging to 26.5 million U.S. veterans stolen in 2006 is one example. A government employee had this data on disks at his home. Another example in England is that a laptop was stolen from a secure area in a hospital. The laptop contained personal data for over 400 patients. The hospital states that their computers are enrolled in a program which is meant to encrypt PCs and laptops. Unfortunately this laptop was not encrypted yet when stolen. Such thefts may lead to what the individual human might fear most when it comes to cyber crime; identity theft.

There are several incidents of identity thefts every day. According to FTC (Federal Trade Commission), 10 million Americans are victims to this every year. Often, the only thing you need for stealing someone's identity is their social security number and name. This can easily be found by stealing their mail or even more unnoticeable going through their garbage. With this information you can change postal address to the victim, order credit cards, rent a car and much more. Catching the thief himself can actually be easier than re-gaining the trust to banks and other companies the thief has fooled while being you.

There are already well known ways to implement encryption of disks. Companies like PGP, PointSec and SafeBoot offers full-disk encryption software. But with this software it also come a lot of work for the system administrators. The software must be purchased, managed and so on. Maybe that is why many companies still do not use encryption on their hard disks.

This January, a company named TCG (Trusted Computing Group) presents three new standards for encryption on hard disks. What differs these types of encryption from what already are available is the implementation. These new standards are hardware based encryption. This means that there is no need for installation of additional software to encrypt the data.

Opal is the name of the encryption standard for notebooks and PCs. For data centers the other standard is called Enterprise Security Subsystem Class Specification. The last standard is Storage Interface Interactions Specification, which describes how these standards interact with other standards for storage interface. PATA and SATA, SCSI SAS, Fibre Channel, and ATAPI are all supported and the vendors of the disks can choose from AES (Advanced Encryption Standard) 128 or 256-bit encryption.

With this information in mind, and the fact to some vendors already offers FDE (Full Disks-Encryption), one might think that software disk-encryption eventually will disappear. Especially when considering the downsides of FED. Robert Thibadeau, chairman of Trusted Computing Group, says that the lack of performance of the disks is virtually none. Analyst Jon Oltzik from Enterprise Strategy Group estimates that in a few years the cost for making the disks will be reduced to almost nothing. Hopefully that will be the truth.

All the work that is reduced with encrypted disks coming directly from the factory, like installing software, update software and manage the software, will probably in time lead to a lot higher use of encrypted hard disks. Not only in the corporate world, but also for the home user. With this, the possibility of security breaches due to stolen disks will sink like the Titanic.

SOURCES

- [1] Hard Drive Makers Develop Opal Encryption Standard For Computer Drives
<http://www.cdrinfo.com/Sections/News/Details.aspx?NewsId=24744>
- [2] Trusted Computing Group outlines new specification standards for storage encryption
<http://www.scmagazineuk.com/Trusted-Computing-Group-outlines-new-specification-standards-for-storage-encryption/article/126599/>
- [3] TCG spec to be foundation of storage encryption
http://news.cnet.com/8301-1009_3-10153007-83.html
- [4] FBI reporter stjal identitet
<http://www.nrk.no/programmer/tv/fbi/1.5532982>