A QUICK LOOK AT THE FUTURE OF PROTECTION – NINE GUIDELINES TO FOLLOW

Alex Tabusca, Ph.D. Candidate Lecturer,
Romanian-American University

With the worst part of the economic crisis gone – at least I hope so ☺ – we can clearly conclude that, despite the real downturns and dropping revenues all over the IT business environment, the information technology did not stop its progress – quite on the contrary, has even developed and launched new and more advanced solutions within both software and hardware fields.
I think it is enough to mention the hardware specialists of INTEL with their new i7 processors family, a very significant evolution if not quite a real revolution, with the Atom series of processors dedicated to netbooks and MICROSOFT with their newest offerings on the operating systems market: the Windows 7 and Windows 2008 Server, with all their different flavors.

The security is of course still a dominant priority and a constant pain producing issue for all players of the IT field, regardless of their stature as simple users, programmers, integrators or large software developers. This fact is – it was and it will be at least for the foreseeable future – a statement backed by the mere reality of the large number of threats and vulnerabilities creating a continuous risk increase on the IT stage.

After reading, studying and even "fighting" some of the theories related to this field I can make up a list of the most important – as from my point of view - security related themes and issues, elements that started to make their way to the stage this year or that have been brought to the specialists attention during the previous years but became significant to the large public only during the latest period of time.

A. Development of Secure Software

Last year, during 2008, the majority of malicious code attacks were targeted mainly at software applications and not the operating systems. This fact, combined with a growing accent put on cybernetic security I think will force the software developers to embrace secure software development efforts initiatives, such as the Open Web Application Security Project (OWASP) or the SANS Software Security Institute. Despite the "ancient" fuss about Microsoft's operating systems vulnerabilities the company and its Pro Network partners, e.g. Security Innovation, are in the best position to bring secure software development best practices to the large public.

B. The Management of Entitlement:

Authentication gets a user on the "door" of the network, while entitlement management gives you the opportunity to do or not to do something. Entitlement management is now performed on an application-by-application basis but this direction does not work for a scaling scenario, is prone to human error and is almost impossible to audit for full compliance. Nowadays we can see some new centralized entitlement management solutions brought by well known names of the IT filed: Cisco, IBM, or RSA Security. I think we can expect a lot of news and projects based on this issue. I also think that in the near future we will see the rise of a new programming language – the XACML, the acronym for XML Access Control Markup Language.

C. Security through Virtualization

We can see now a proliferation of server and desktop virtualization solutions but this trend needs to be accompanied by better security tools in order to increase the protection offered on the lines of role-based access control, virtual server identity management, virtual network security, reporting and auditing. Microsoft, VMware and Citrix will most probably remain in the lead for this effort with partners able to provide support from others great names like IBM, Symantec, McAfee, Softwin or Kaspersky Labs.

D. Cybernetic Security Issue

The 2009 year has begun with the United States establishing the Comprehensive National Cyber-security Initiative (CNCI) -as an effort to strengthen official networks. think this solution was a very good one – as obviously the US is the usual leader of the field – but due to the unfortunate economic crisis the funding and support received were very low. The US President seems to have found a solution – in may 2009 – by appointing a well known name of the field in charge of the initiative and by finding a solution to fund it through a public-private partnership, stating that the initiative will develop into a cooperative intelligence and law enforcement solution with a continuous growing list of other nations.

E. The Evolution of the Endpoint Security Concept

Some articles and specialist have declared that antivirus software is on the verge of extinction, sort of a dinosaur's end ☺. Personally I disagree with that; I think that endpoint security is just developing as a function of the changing threat landscape.

I expect that classical antivirus solutions, anti-spyware, anti-malware and firewall software will merge together with endpoint operations and actions, data loss prevention, data recovery and content encryption.

The Symantec Endpoint Protection package of Symantec seems a great solutions – by the way, I use it as both everyday corporate and home solution and it is one of the best tools I have seen in over 15 years since I started crawling around the PC universe ☺.

F. Ubiquitous Encryption

The most modern encryption technologies are now usually becoming "default" rather than "add-on". Nowadays tape-drives contain cryptographic processors, the hard drives have encryption utilities and even the all around USB toys that every kid uses have encryption capabilities and support. Hardware giant Intel is now beginning to ship a new version of its vPro chipset that also supports onboard encryption. During this year I think we will see multiple different layers of encryption technologies running together and on top of each other, enveloping our old files like some sort of a protective cocoon.

This solutions are all good for data confidentiality and integrity but they will also highlight again the need for enterprise-class encryption key management.

G. The Increase in Security of the Business Process

Starting with a medium-sized company specialists consider that we have to secure all IT assets across the enterprise – and this is a daunting task. Rather than rely on IT reports and security point tools alone, most modern executives will want more visibility and oversight over their exclusive domains with detailed and succinct portals, reports, auditing and alert systems. Ultimately, the general managers will support this effort as it forces individual business units to build security into their own "inside fabric". I think this trend will favor the large services vendors like DELL, CSC or HP with their comprehensive vertical industry tools, business process expertise, and executive relationships.

H. Cloud Security

While the word "cloud" has had different meaning during the latest years, turning into quite a vague industry security term, I think that 2009 will bring a new trend for managed security services. Most companies do not have now the budget money or the security skills and knowledge to take on the increasingly sophisticated attacks by themselves – this fact is some sort of great news for others, like Symantec, IBM or McAfee. Moreover, even other 2nd tier companies in this field, like Cisco or Trend Micro will supplement on-site security equipment with scalable reputation and update services in the cloud.

I. Security Centered on Information

I think that the recent joint Microsoft-RSA announcement is a sign of things coming our way in the near future. Companies, regardless of being large, medium or small, need to be able to discover and classify sensitive information, apply security policies, and then enforce these policies throughout their entire network. This will continue to become a reality in 2009 as more and more documents and file systems are integrated with data loss prevention, recovery mechanisms and enterprise rights management systems. I think one of the next steps in this direction will be the introduction of PKI in this security mix along with new metadata standards for data classification and security rules enforcement.

I do not even presume to have mentioned all the “hot” trends of the present IT security field but I am confident that, among the ones I missed, my chosen issues will be significant for the development of a new and more protected cybernetic space.

Most probably there will be problems and issues – they have always been and they will always appear – but, despite a lot of gloomy predictions I read about “certain” catastrophic event in 2009 - well, from the IT security perspective at least – I think that security grows stronger every day. With the introduction of the quantum-related technologies to the public in a few years I think that most content transportation and encryption issues will be solved and we will have to think about other threats and others ways to protect from them.