Endpoint security: "Essential security" or "Impossible dream"?

Smart phones and other holiday gifts raise device security questions anew

The Jericho Forum By Paul Simmonds, Network World, 12/12/07

Simmonds is a member of the management board of the *Jericho Forum*, an organization pushing for innovation in e-commerce *security*, and is also chief information security officer for a large, global chemicals corporation. Here, *Simmonds* speaks out on the topic of endpoint security.

It's that time of the year. Many employees will receive gifts during the holidays that will impact your network perimeter and security. Of course, we are referring to the millions of new smart phones, laptops, and other mobile devices that will come with requests to be connected to corporate networks following the holidays.

Actually it doesn't really matter whether it's a personal device, or a corporate push for "consumerization" as a cost-saving measure. Are we, as IT security practitioners, fully prepared to protect our businesses against the ever increasing number of devices that are creating new entry points into a once-tight system, and further eroding our perimeters?

It's not just the personal devices - it's about the business requirements needed to connect users to our systems, both business-to-business (B2B) and business-to-consumer (B2C), including consultants and contractors who bring with them their own laptops. Companies, such as BP and KLM/Air France, for instance, are exploring giving staff "PC allowances" to buy and support their own IT equipment. All these devices are placing new demands on business' capability to provide trusted access to services.

As IT security leaders, our job is to marry security with business needs - in this case, to define and implement end-point security measures that enable our companies to achieve optimum results by securely conducting business in an open-network, mobile world.

The Jericho Forum believes that end-point security is about raising the level of inherent trust in computing devices, to a point where all the devices involved in any transaction meet the criteria of trust required for that transaction. Simple to say, but the technologies to achieve this are severely lagging.

The "old" model whereby an organization is going to dictate how every end-device is going to connect, and specify both the end-point software and network hardware standard is flawed in all but the smallest organizations. In any reasonable size organization, the likelihood of being able to mandate that all (internal) network connections are on the latest network hardware capable of supporting Network Access Control (compare products) is exceedingly unlikely.

In addition, we need to ask - is there client software for every type of client you want to connect to your network? And, don't forget the Linux systems, the multi-function photocopiers, the Windows NT devices and your obsolete factory control systems. Now what about all those mobile devices and "toys" that everyone received as presents… and all this is assuming that you can mandate fitting the software in the first place, because your home users are not likely to want corporate mandated security software on their own PC's (or Macs). Remember security is only as good as your weakest link.

The Jericho Forum believes that for two points to securely transact with each other there needs to be a level of mutual trust. Yet today, after years of discussion and debate, end-point security is too often limited to one-way trust – validating clients trying to connect into "your" environment without enabling the client to have the opportunity to validate you. This leaves corporate networks extremely vulnerable to malicious attacks, including phishing.

The only way to ensure secure transactions is to establish mutual trust by authenticating the client end-point to an organization's network and the organization to the end-point. Being able to establish this level of trust allows more valuable transactions to take place electronically in a de-perimeterized environment. Two-way trust is of paramount importance to properly authenticate, validate and enable secure interaction.

Organizations also need to be able to register end-points from many sources – their own, customers, suppliers and mobile workers. At the same time, end-points need the capability to be registered in several security zones. User agents must be able to access user credentials, tokens, end-point credentials and posture-checking agents, while access managers need to make access decisions based on both the user and the end-point attributes.

To accomplish this, we need open standards, which will guarantee interoperability for end-points with single security agents from multiple vendors. Likewise we need open standards for secure protocols designed to allow end-point security agents to be safely validated by remote end points. Open standards in these areas will enable various types of end points – including smart phones, PDAs, network devices and all PCs - to safely interact.

The Jericho Forum believes that, as business demands, to allow remote connectivity and cross-organization collaboration in a de-perimeterized environment, we have to be able to trust remote and mobile end points. The industry needs to turn its attention to creating open standards that allow many types of clients to authenticate at both ends of the transaction without needing matching software all from the same vendor.

Unfortunately, while this may be on the priority list for corporate IT professionals, the vendors do not see it as their priority, and there seems to be little sign of tangible product in this area. But at this time of year we can still dream…after all, maybe Santa Claus will deliver it.

Ten questions to ask yourself if considering end-point security:

1. Is your entire network hardware NAC-ready, or how much will you have to upgrade?
2. Does every endpoint support 802.1X for authentication?
3. Does every endpoint have agent software installed at a suitable level?
4. Can you get agent software for the myriad of devices you own?
5. Can you enforce your standards on everyone who connects to your network?
6. How will you handle legacy devices?
7. How will you handle third parties, business partners or home users who want to come in from outside?
8. Can you leverage your existing organizational authentication systems?
9. Does this organizational authentication system cover all your devices (or just Windows)?
10. Can you make a business justification for the total cost of your project?