CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Evolving Business Models, Threats, and Technologies: A Conversation with CERT's Deputy Director for Technology

Key Message: Business models are evolving. This has challenging implications as security threats become more covert and technologies facilitate information migration.

Executive Summary

As businesses become more globally interconnected with their partners, suppliers, vendors, and customers, the business model is shifting such that the network is becoming the business. This means that boundaries between organizations, including the ability to control and protect information at a known location, are disappearing. Security threats are becoming much less visible and covert, "below the radar." They target the disruption of business processes, information flow, and trust relationships. Technology solutions that facilitate this evolving business model present new opportunities and new threats.

In this podcast, Tom Longstaff, CERT's Deputy Director for Technology, discusses how business models are evolving and the implications for security threats and technology solutions.

PART 1: EVOLVING BUSINESS MODELS; EVOLVING THREATS

From Overt to Covert: The Changing Nature of the Threat

Five to ten years ago, the security threat was much more overt and "in your face" than today. This included attacks on your firewall, viruses, and worms, where there were well-identified locations for deploying protective technologies that worked.

The thinking was, "Put some protections in place, monitor your network, and when you see an attack, respond to it." There is a boundary, a perimeter we can fortify to protect the business -- the fortress mentality, with a clear distinction between insiders and outsiders.

This is no longer the case. Today the threat is much more covert, more subtle, more underground. Why?

Today, the Network Is the Business. Everyone with whom you do business (customers, suppliers, partners, vendors) is a node in your network. Nodes exchange information, goods and services, and money in a much more direct way.

Your security is not only dependent upon what you do with the data you own, but also on the limits you impose on what others do with your data, and the limits they impose on you with respect to their data. In other words, there is a high and growing level of interconnectedness and interdependency.

So What Do I Need to Protect?

Business process is the fundamental asset that requires protection (instead of computers, networks, and databases). Business process viability includes knowing that you are interacting with the right people, with verifiable levels of trust, and with clearly stated expectations of one another.

The security question to ask is, "What do I need to do to ensure that my business processes are not interfered with by an unauthorized party?"

Instead of banging on the front door of the fortress, threat now focuses on manipulating business processes to extract

information, change the value of information, steal money, or interfere with the business trust relationships. The true cost of phishing, for example, is not the loss of money but the loss of the trust between the client and the provider.

PART 2: TECHNOLOGIES TO WATCH OUT FOR

Those That Affect Business Processes and the Ownership, Location, and Flow of Information

Watch the evolution of e-mail to web-based services to Ajax (shorthand for Asynchronous JavaScript and XML, a web development technique for creating interactive web applications). This evolution changes who has what information at any point in time, and who controls it. This, in turn, changes who is in charge of a given trusted relationship. Key information can almost be considered to be location independent.

Standards offer some approaches to preserve trust in information and the business processes they support, such as digital rights management.

Standards and agreements evolve in three ways:

- Traditionally and formally through such organizations as the Internet Engineering Task Force
- Through de facto industry standards created by a large install base, such as PowerPoint, PDF, and Excel for spreadsheets
- Through emergence such as that occurring in social networks and other applications that move the data model to the client, for example, Ajax and Web 2.0

The characteristics of emergent technologies include:

- Security emerges with the solution.
- Solutions are defined by a rapid evolution caused by people using the tools and dealing with the threats as they emerge.
- A rapid evolution (by early, savvy users) of threat, response, threat, response, threat, response -- from rudimentary (and visible, loud) to sophisticated (quiet, covert) in 18 months or so.
- Businesses adopt those that survive this evolution, which increases available, lucrative targets and thus the threat level.

PART 3: ACTIONS LEADERS CAN TAKE

Questions to Ask to Help Prioritize Protection Actions

- Where is my information?
- How is it being protected?
- How are my business products being protected?
- How do I state in whom I trust and what I trust them to do?
- What does this all mean in terms of a protection model?

Trust is essential. If trust breaks down, it is very difficult to stay in business.

Eventually, all businesses will need to adopt a more open business model to survive and thrive in a globally competitive marketplace.

Example: The Power Industry

- Historically, this industry has not relied on the Internet in any significant way, but this is changing in large part due to deregulation.

Operating in an open marketplace, components of the industry are competitive with one another yet need to cooperate to distribute and manage power.
- For example, marketing (who buys and sells) needs to be directly connected to operations (to determine current state).
- The power industry did not understand the implications (and changing threat) due to this open, interconnected marketplace.

The more we operate as virtual, interconnected enterprises, the more everyone becomes an insider.

Resources

Hernacki, Paul. Web 2.0 for the Rest of Us. TechLinks, November 14, 2006.
