Information Security Savvy with Dr. Eugene Schultz

Entrevista a una de las autoridades mundiales en el tema central de esta edición.

Dentro de las actividades que se ha propuesto la Asociación Colombiana de Ingenieros de Sistemas (ACIS), figura motivar el uso del inglés entre sus afiliados. De ahí la decisión de publicar esta entrevista en ese idioma, sin traducción al español.

El entrevistado Eugene Schultz, es experto a nivel internacional en temas de seguridad de la información. Tiene una amplia trayectoria en temas relacionados con sistemas UNIX, Windows, Redes LAN y seguridad en Bases de Datos. Ha sido consultor en la industria privada y para el Gobierno norteamericano.

El Doctor Schultz fundó y administró el centro de atención de incidentes del Departamento de Energía de los Estados Unidos de América; es co-fundador del Foro de Respuestas a Incidentes y equipos de seguridad, conocido a nivel internacional como el FIRST.

En el ámbito académico ha formado parte de centros de investigación en universidades como Purdue University; partícipe de estudios en el CERIAS (Center for Education and Research in Information Assurance and Security) en USA, y como docente de la Universidad de California (Berkeley Lab) en Estados Unidos.

Obtuvo su grado doctoral (Ph.D) en Ciencias Cognitivas en Purdue University en 1977. Actualmente es Chief Technology Officer de la empresa Emagined Security, con sede en San Francisco, Estados Unidos, dedicada a los temas de consultoría en Seguridad de la Información.

RS: SIEM technologies are really effective to fight against information insecurity? Could you please explain your answers?

ES: SIEM tools do not by any means solve all security problems, but they are an effective defense method in a "defense-in-depth" strategy. A "defense-in-depth" strategy means deploying numerous layers of security, such that if an attacker defeats or bypasses one layer, other layers that can deter the attack will still be present. For example, SIEM technology provides a means of identifying and responding to attacks that might otherwise be missed by intrusion detection and intrusion prevention systems. Today's cyberattacks tend to be small and subtle in order to avoid detection by intrusion detection systems and system auditing. Many commercial SIEM tools have event correlation capabilities that can identify, link together and report small and subtle events. Additionally, many SIEM tools have built-in incident response facilitation functionality to help those who respond to incidents to follow their organization's incident response procedures, archive potential evidence, and work with each other as cooperatively and efficiently as possible.

RS: In your experience, how is the best strategy to implement SIEM technologies in organizations? ¿What's critical success factors to be consider?

ES: I am not sure if one best strategy exists. Those who use SIEM tools have different requirements and different network topologies, leading to different deployment strategies. All things considered, however, one of the best ways to deploy SIEM tools in large network environments is to have individual SIEMs in various parts of each network, and then to set up a master SIEM to which all data received by each individual SIEM are sent. Consequently, all the information is available at a single location, something that greatly helps in understanding and reacting to security-related events throughout an entire enterprise.

One of the biggest critical success factors in SIEM technology is buying the right SIEM product for an organization's security needs. SIEM technology is actually a combination of SIM (Security Information Management) and SEM (Security Event Management) technology, but some SIEM products are much more SIM than SEM-like in nature. The opposite is true for other SIEM

"..Unfortunately, many SIEM vendors too often overstate the functionality of their products..."

products. If you need log archival, management, and reporting more than anything else, you should buy a product that is more SIM-like. If you need intrusion detection, event correlation, and incident response, you should a SEM-like product. From what I have seen, many organizations have SIEM products that do not really meet their needs very well. They often end up scrapping the product that they have bought, forcing them to looki for and eventually buy another one—a gigantic waste of time and money. Additionally, some SIEMs have much better functionality than others. Unfortunately, many SIEM vendors too often overstate the functionality of their products, so systematically and thoroughly testing each candidate SIEM product is essential.

RS: What new technologies or strategies do you see in a near future for Information Security Management?

ES: The current global economic slump is slowing down the development of new technology, so I do not foresee many new types of security technologies surfacing in the next few years. But I expect the current trend of firewall screening of incoming network traffic primarily at the application layer to continue to grow. Application firewalls will become increasingly sophisticated in recognizing and stopping attacks that target applications. I also expect intrusion prevention as a standalone technology to go away; it will instead be incoporated into other network devices (e.g., blades) as an add-on functionality.

RS: Cybersecurity is now a top priority for US. Considering this issues, what recommendations do you have for Latin American countries based on this issue?

ES: I'd recommend using the information security governance model that the Information Systems Audit and Control Association (ISACA) advocates (see www.isaca.org). Information security governance means (among other things) planning a strategic direction and goals for an information security practice and then ensuring that necessary mechanisms are in place and working properly to

ensure that the direction and goals are met. The direction and goals must be based on and aligned with business drivers—security must support, not hinder, whatever direction the business of an organization is headed.

RS: The human factor is critical issue for information security management. In this sense, do you see important changes in this factor to promote secure behaviors in organizational process? Please explain your answers...

ES: Yes, information security is really more about people than anything else. People have to do the right things and avoid doing the wrong things (e.g., opening email attachments that they have not been expecting, even if the attachments appear to be from something they know) if security is to be effective. People must know what is expected of them, something that an information security policy must clearly convey, and they must also know the consequences if they do not act in accordance with the provisions of their organization's security policy. One of the long-range goals of an effective information security practice should be to develop a "security culture," an environment within an organization in which people value security and willingly act in accordance with security requirements because they understand why security is necessary.

RS: What's your "tips and tricks" for chief information security officers in Colombia?

ES: As I mentioned earlier, use an information security governance approach. Form close working relationships with top-level management; learn what their goals and expectations are, and then mirror them in your information security practice. As I also mentioned earlier, adopt a "defense-in-depth approach in deploying security measures." Use the appropriate types of information security technology, but do not rely on technology to solve every problem. Institute a rigorous change control process that not only assures that critical information technology and other changes are approved through a systematic process, but also that anticipates and addresses new secujrity risks that change invariably creates. And because information security is more of a people problem than anything else, devote a disproportionate amount of resources and effort to information security training and awareness that targets *all* groups---managers, users, system administrators, application developers, and others, not just users—within your organization.