Incident Response - Stopping Them Dead in Their Tracks

Chair -

Jon David
Lehman Brothers

Panelists -

Robert Stone
UUNET Technologies

Jim Duncan
Cisco

Bill Hancock
Exodus Communications

Richard Reybok
Vice President Direct Markets
Merrill Lynch

When security fails, as it always has done and will always continue to do, reaction to breaches is of prime importance. This session defines incidents, tells what you can -- and can't -- expect from your ISP and other upstream providers, gives a real world approach to actual responses, and discusses the involvement of others, from local through an international level, as necessary.

This is the first of a double session on Incident Response. The second session, chaired by Dr. Bill Hancock, will immediately follow this one. The emphasis in this session will be stopping whatever activities have caused the incident, and the next session will treat tracking down of the causes.

In particular, we will deal with incidents of internal and external origin, the sorts of plans that have to be in place to reasonably respond to an incident, what to do when it looks like a goodly part of the problems are due to remote (out of locality, out of country) individuals/facilities? How can we stop the immediate/ongoing harm, yet not [too badly] destroy evidence?

Jon David

Jon David is an officer in the Security Engineering group at Lehman Brothers. With over 30 years in security, he was a pioneer in both computer and network security. Prior to Lehman Brothers, he was Director of Network Security for an ISP, and spent a depressingly long time as a security consultant. He is a frequent author and speaker, and has repeatedly been in the van of security technology. Well past his prime and clearly at the pre-dotage stage of life, he lives off of the knowledge and abilities of friends these days. In an attempt to disguise his street kid tendencies, he did his undergraduate work at Queens College and his graduate work at Columbia University.

Robert Stone

Robert is the Security Architect at UUNET Technologies, Inc. In the past four years, Robert Stone has participated in a number of projects at UUNET including VPN product design, backbone AAA system design/implementation, design of the CenterTrack DoS tracing mechanism, and the creation of a number of intermediate DoS tracing and countermeasure solutions. He has also assisted with a number of incidents including the February DDoS attacks and others which can not be mentioned here. Currently he is working with others in the industry to research DDoS tracing and prevention solutions. When he is not working he enjoys driving his sports car, riding motorcycles, swimming, and windsurfing.

Jim Duncan

Jim is Manager for Cisco's Product Security Incident Response Team (PSIRT), responsible for assisting customers with network security matters. Prior to Cisco, he was associated with the Penn State CERT. A contributor to the Site Security Policy Handbook (RFC 1244), he has written many security advisories, policies and guidelines dealing with system and network administration, and with security incident handling.

Bill Hancock

Dr. Bill Hancock, CISSP, is the Vice President of Security and Chief Security Officer of Exodus Communications, Inc., a worldwide leader in complex Internet hosting, networks and security solutions. A well-known network and security consultant, designer and engineer with thousands of network designs and hundreds of hacker/cracker trackdowns to his credit, Bill has "been there and done that." An expert on networking, security and e-commerce and its various implementations, Bill has been involved in the design and implementation of some of the most sophisticated e-commerce systems in the world such as travelocity.com and the Internet backbone networks. He is often seen on-CNN, ABC, BBC, NBC, FOX and other networks as an expert on security, networking and the Internet.

Bill has written 28 books on computer networking and security, currently writes a regular column in Network Security magazine and is Editor in Chief of Computers and Security Magazine. He is also a U.S. network expert to the ISO and sits on various standards committees. Bill is recognized in Who's Who in the World, Who's Who in Science and Engineering and Who's Who in Finance and Industry. Bill is a member of many industry societies (IEEE, ACM, DECUS, ANSI, etc.) and has sat on the boards of several organizations. He is a Certified Information Systems Security Professional (CISSP), Certified Network Designer (with Architect Endorsement), Certified Systems Analyst and has earned a B.A., M.S. and Ph.D. in Computer Science.

Richard Reybok

Richard Reybok has worked in the financial sector for over five years as a security analyst. During that time he has been responsible for front line incident response of data theft, corporate espionage and true hacking incidents. He has helped to develop incident response teams in some of Wall Street's largest fortune 500 companies.