



STORES[®]

November 2005
www.stores.org

DATA SECURITY

Curing Data Breaches

HoneyBaked Ham implements **Intrusion Protection System**

BY DAVID P. SCHULZ

Protecting customers' personal information is not just good business; it can also help avoid costly fines. Breaches of retailers' customer information databases have been well-publicized. In one case, a wholesale club operator had to pay \$10 million and agree to allow third-party audits every two years for the next 20 years [See sidebar].

Other retailers don't want to be put in a similar situation.

According to the credit card processors, "We are not a top-tier company" in size or sales volume, says Erik Goldoff, information technology systems manager of HoneyBaked Ham Co. "For a first-time violation, we could be fined up to \$50,000 and if the violation isn't corrected within 60 days, \$10,000 a day not to exceed \$500,000. That's a lot of money."

Goldoff says Norcross, Ga.-based HoneyBaked Ham decided to implement an intrusion protection system (IPS) rather than an intrusion detection system (IDS) on the network carrying information between headquarters and some 350 company-owned and franchised stores.

The difference, Goldoff says, is that an IDS tells you what has just happened; an IPS detects and prevents intrusion, "which is a much better choice."

The impetus for making the move was the Payment Card Industry [PCI] Data Security Standard bulletin jointly issued in December by credit and debit card issuers. The document includes a series of requirements designed to protect cardholder data that apply to all members of the card-issuing associations, merchants and service providers that

store, process or transmit cardholder data.



HoneyBaked Ham decided to implement an intrusion protection system on the network carrying information between headquarters and some 350 company-owned and franchised stores.

Exploring solutions

To meet these challenges, Goldoff investigated a number of potential solutions. He described one as being an IDS running on a PC operating system, “but it doesn’t handle the bandwidth” and “it could result in [false] denials of service.” Another potential solution required the backward creation of a database and the installation of an agent on any device to be protected.

“We didn’t want an IPS security solution that would effectively cause our own denial-of-service situation,” Goldoff says. “That’s one of the security events we’re trying to prevent, not implement.”

In addition, both of these systems were software-based, a negative in Goldoff’s opinion because that could lead to network degradation.

His choice was the IPS 5500 from Westboro, Mass.-based Top Layer, which was purchased through Vigilar, an Atlanta-based reseller.

The Top Layer IPS 5500 is a dedicated piece of technology deployed on the perimeter of the data network that works at very high speeds.

It also offers validation modules that use protocol anomaly detection to inspect all transactions for acceptable use of the appropriate protocol so that exploitation of most critical vulnerabilities are automatically blocked, regardless of the attack method.

While most intrusion-detection systems look at the source of the data,

WHOLESALE CHANGES

BJ’s Wholesale Club, the \$7.4 billion retailer based in Natick, Mass., paid the price for failing to encrypt customer data transmitted or stored on its IT system, using default passwords to access the data and operating poorly monitored, insecure networks.

The charges were laid down by the Federal Trade Commission after counterfeit credit cards were created and used based on data retrieved from BJ’s network.

“Consumers must have the confidence that companies [that] possess their confidential information will handle it with due care and appropriately provide for its security,” says FTC chair Deborah Platt Majoras. “This case demonstrates our intention to challenge companies that fail to adequately protect consumers’ sensitive information.”

In the settlement, BJ’s agreed to pay \$10 million over a two-year period and to implement an upgraded data security program subject to third-party audit every other year for 20 years.

Goldoff says, the IPS 5500 “looks at the content and looks specifically for exploitation characteristics.” In comparing IPS versus IDS, Goldoff says the former is “a lot more intelligent.”

Proof positive

Turning to the question of how to measure the performance of the IPS 5500, Goldoff says “there are over 125,000 dropped malicious packets on any given day, just looking at it quantitatively.”

Defining payback of the device provides a different type of challenge. As with anything in security, Goldoff concedes, “If it doesn’t generate revenue, it winds up becoming part of the overhead.”

The installation of the IPS on the data network has not created any extra work or procedural changes at store

level. “They don’t have to do anything different,” says Goldoff, who describes the company’s data-gathering system as a “wheel, hub and spoke configuration” that results in the IPS generating some additional duties for the IT staff. “That’s not necessarily a bad thing,” he says.

The IPS 5500 has been in place for less than a year, but Goldoff doesn’t anticipate any problems when payment card transactions pick up during the holiday selling season. While he couldn’t provide a breakdown of cash vs. payment card use, Goldoff indicates that, “During the holiday season, when people are buying gift orders and entertaining, a larger portion of the transactions are via payment cards.”

Though the IPS still has its heaviest traffic loads ahead of it, it has performed well so far. “It’s exceeded our expectations,” Goldoff says.

Goldoff compares the configuration of HoneyBaked Ham’s IT network to a professional football team. “You may have the best quarterback in the league, but that doesn’t mean you have the best team,” he says. “We try to get the best player for each position. Top Layer was the best player at its position.”

David P. Schulz, a New York-based writer and editor, reports on U.S. and foreign retailers for several publications.

“The IPS 5500 looks at the content and looks specifically for exploitation characteristics.”



— Erik Goldoff, information technology systems manager, HoneyBaked Ham

www.TopLayer.com
508.870.1300