

The Heartland debacle, take one

Government Security News

Jan 29, 2009

By now, you have all heard about what may be the largest security data breach ever. Heartland Payment Systems, a large payment processor, was the "victim" of a data breach which may have exposed more than 100 million credit/debit cards (of course the real victims are the people whose credit card data was compromised). It is believed this compromise took place over a period of four months. The sheer numbers are staggering.

Of course, those of us in the public sector are no strangers to data breaches. In the recent past, there was a steady parade of government entities making headlines about a misplaced/stolen laptop, or data that was somehow exposed and compromised. These types of incidents and the ill-gotten gains that result are the true casualties in cyber security wars. In the government, the stakes are even higher.

Besides financial motives, there are other reasons for trying to access information contained on our government networks. All too often, information security and IT professionals are hiding behind the veil of compliance. In doing so, they fail the ultimate goal of securing the network and the data that resides on it. In too many sectors, including the public sector, compliance has trumped best practice security processes. Whether we are talking about FISMA, HIPAA, GLBA, PCI, etc., our pursuit of passing the audit has become the primary goal.

The Heartland case is a perfect example. They had a full PCI audit and were certified in April of 2008. According to reports, the Heartland team became aware of a potential breach as early as last October and did not detect malware on their systems until January 2009. According to PCI compliance guidelines, Heartland had to undergo quarterly compliance scans. Assuming that the malware was not installed until October (it may very well have been there longer), Heartland had one or probably two audit/scan cycles while they were infected and compromised. They were supposedly PCI-compliant yet they still managed to be compromised, which resulted in tens of millions of credit card transactions being exposed each month.

Heed the lesson of Heartland. Compliance is not a substitute for security. Yes, passing that FISMA/PCI/HIPAA –take your pick -- audit is important. But security rules, statutes and regulations are almost always based on sound, common sense security principles. Do not be lulled into a false sense of security, remain vigilant of any suspicious activity and do not hesitate to institute best practices just because they may not specifically help you pass your next audit. Remember: the data you save may be your own.