

WHEN ALL ELSE FAILS...

BY DUANE VERZONE, CISSP

You addressed everything. You have firewalls in place, IPS devices are monitoring all your network segments, anti-virus software is running on all systems, including one that specifically monitors the email gateway, and your periodic penetration testing has allowed you to remediate all of the vulnerabilities found in your network. So, how is it that you find yourself on a Friday, with month-end processing piled to your ears, fighting what appears to be a combination of a virus, a distributed denial of service, and an adware explosion on your network?

Welcome to the world of the zero-day attack. Zero-day exploits are released before or on the same day that a vulnerability or vendor patch is made available to the public. The term derives from the number of days between the public advisory and the release of the exploit.

Be assured that you have done everything you could to prepare for this event. However, now that the crisis is over, management has some challenging questions:

1. Was there a compromise of member/client data during this threat?
2. Was the **<Fill in your most recent network security purchase>** supposed to keep this from happening?
3. Why did **<Fill in one of your security vendors>** not make us aware of this?
4. Who is responsible for this getting on the network in the first place?

Answering these questions is going to make you the stalwart hero, or get you a serious roasting. That being the case, here are some issues you need to address before you find yourself in this situation.

The correct answer to Question 1 needs to be either yes or no. You hope the answer is no, but if it is yes, you must be able to provide a list of all members/clients whose data was affected. The only way to guarantee your answer to this question is by ensuring you have a logging framework in place that will identify the extent of systems compromised and data accessed. Log files and the infrastructure to protect log files are frequently overlooked facets of the network security world. The SANS Institute has espoused, "Prevention is ideal, but detection is imperative" to emphasize this point among security professionals. Do your log files contain enough detail and reliability to answer questions addressing data compromise?

Question 2 examines the effectiveness of the last software or hardware purchase for network security. It is your job as the organization security expert to inform management that although technology can assist in preventing intrusions, it cannot eliminate them entirely because the software/hardware is only as good as its most recent upgrade. No matter how good the new 'wiz-bang gadget' is, it cannot protect you from the zero-day attack. It is a good idea to educate management by making them aware of the lurking specter of the zero-day exploit. Does your management understand that technology does not equal security?

Question 3 implies responsibility relies outside the organization. Security vendors are also unaware of zero-day attacks in advance. The perception that security vendors have access to 'privileged' information to which the masses do not have access is inaccurate. The majority of exploit development today is done deliberately with the specific purpose of either stealing money, or the means to acquire money in the form of credit card numbers or personal information. The days of the altruistic hacker

have come and gone. A large part of the benevolent hacker community now works for legitimate security vendors trying to develop the next zero-day fix before the criminal hacker community releases it. If they are successful, warnings and patches can be in place before the zero-day exploit arrives.

The criminal element craves and desires the money, credit card numbers, and personal information of your members/clients. They are willing to work diligently and patiently to acquire that information. The weakest link in the security framework is always people. Training people not to open seemingly benign emails from unknown senders, not to randomly browse websites sent by their family members, and to be suspicious of phone calls from people who claim to be from the IT department, all seem like common sense things to do. The reality is that the average person will open an email if they think it might prove interesting, browse to a website simply because one of their family members sent them the link, or willingly follow the instructions of the person on the other end of the line if they believe they are going to help them fix some type of computer problem. Would your people do the same?

So, now that the crisis is over, are you ready for the questions posed by management?