BE FREE

CASE STUDY

BE FREE OF RISK

Operations Down: Solving a Security Breach

A medical device supply company suffered a major security breach that shut down operations. BestIT solved it.

Briefing

Computers at a medical device supply company were infected with a worm that caused operations to completey shutdown temporarily. BestIT immediately responded to the breach and flew the security SWAT team to the company take care of the situation and reinstate business operations.

BE FREE

Operations Down: Solving a Security Breach

Client
Medical Device Supply Company

Industry
Healthcare Equipment

Challenge
The client, a medical device supply company, discovered that its entire computer network had been breached by an infection that its anti-virus controls did not detect. The CIO at the company called BestIT to help them figure out the how much of the network was compromised and if any sensitive information had been stolen due to the breach.

Services Provided
- Response and Containment
- Forensics
- Recovery

Introduction

Having an anti-virus system in place is not enough to keep your company systems secure. New viruses and security vulnerabilities are discovered frequently and if your system's anti-virus software isn't up-to-date, security breaches will often slip through the cracks. No security strategy should rely solely on anti-virus and firewalls—enhanced security tools and practices need to be put in place for an effective and efficient IT security infrastructure.

The Problem

The client, a medical device supply company, discovered that its computer network had been compromised by a virus that its anti-virus controls did not detect. The IT department at the company called BestIT to help them figure out the how much of the network was at risk by the virus and how to clean it up. BestIT immediately flew out to the client's headquarters to determine the extent of the security breach.

BestIT began to perform an analysis on the computers and determined that the infected machines were creating copies of infected files on the hard drives of the network. A member of the IT team at the company had successfully identified a few of the malicious files and deleted them but it wasn't working. They were duplicating and re-infecting the machines too quickly. BestIT determined it was a worm that infiltrated the systems. In addition, the CIO at the organization was concerned that the worm had been deliberately put onto the systems.

The Solution

All computers connected to the network were unplugged and turned off for the day aside from a few that were known not to be infected. Most of the IT staff was relieved while BestIT worked out a solution to the security breach. First, the anti-virus definitions needed to be updated to include the new worm that wasn't being detected. BestIT got in touch with the anti-virus provider and notified them of the gap in their virus scanning software. After four hours of going back and forth with the company, BestIT security experts were able to prove to them that the virus wasn't being detected with their software by sending them an example of the worm in a zipped file from a USB stick. The anti-virus company sent out an update to include the new threat for all customers. Once the anti-virus definitions were properly updated on the systems, BestIT worked to clean up the network drive until it was certain that no new computers were being infected. Infected computers were separated and placed into quarantine. The CIO at the organiza-

tion was concerned the containment process was interfering too much with normal business operations. BestIT had to take the infected files off the floor, reimage spare computers so employees could come in and work on non-infected computers until the breach was completely contained.

The final step of the breach was making sure no important information was being leaked during the breach. BestIT took a copy of log files from before, during and after the breach for analysis. A forensic image was made to see what the computer virus had been up to.

The Results

BestIT traced the origin of infection to an email attachment sent by another company that organization did business with. Since the anti-virus program did not initially detect the infected attachment, an employee opened it without being alerted that it contained a harmful file. By the end of the breach response, the medical supply company had evidence that the security breach was not leaking sensitive company data and the breach was not deliberate. A successful quarantine helped the company replace the infected computers with new ones to restore regular business operations.

Benefits

- Restored Business Operations
- Updated anti-virus definitions

Conclusion

The medical device company was able to have peace of mind once BestIT helped them determine that none of its sensitive data was lost during the breach. They were able to recover quickly and the security threat was destroyed. Security breaches are becoming more frequent in this day and age. One way to prevent a major security breach from hitting your company is by keeping your security tools up-to-date and having regular vulnerability testing done to check for any gaps in the system.

Being aware of the vulnerabilities that exist within your system with a security assessment is better than only relying on anti-virus software and firewalls that might not be able to protect your data against advanced and more sophisticated attacks. Contact BestIT today to see how we can help you take preemptive measures to strengthen your security infrastructure or solve a security breach at your company.

Contact us for more information.
BestIT HQ
3724 N. 3rd Street
Phoenix, Arizona 85012

+1.877.222.8615 | info@bestit.com
www.BestIT.com