Recover after an attack

So you’ve suffered a cyber-attack, with your systems and data compromised and your IT department has done all they can to restore the systems to a state prior to the attack. No one’s going to be particularly happy that they were the victim of a cyber-attack, but how do you feel about the way it was handled? Are you worried that there are still vulnerabilities that have not been identified? Do you have confidence that your organisation is more prepared than before - could it withstand another attack?

Restore confidence

Infosec Partners provides organisations with full Cyber Emergency Response services, making sure that your company is well prepared and ready to act in case of a cyber incident or identified attack. This includes the preparation and planning that is so critical in ensuring your organisation is ready and able to respond effectively whether a minor incident or a major emergency.

“We were attacked and tried to fix it ourselves. How can Infosec Partners help?”

Even if you haven’t engaged with Infosec Partners before we can still help even if you’ve already tried to fix it yourselves. The first thing we would do is to make sure you’re really safe from further harm. Then we would take a look at what happened through forensics, scans and interviews to create a comprehensive report you can use. Then it’s a matter of demonstrating lessons learned and being stronger after the event.
Incident Response Services: So you think you’ve been breached?

Post breach, what’s on your mind?

1. Am I still vulnerable?
   Recognising there has been an attack and identifying the cause is vital to containing the damage and nullifying the threat. Attacks are becoming ever more sophisticated and it’s now common practice for one attack to act as a smokescreen for another. Not all attacks are announced and come with ransom notes. Attackers tend to try and stay hidden once they get in to explore then exploit whatever vulnerabilities they can find. Even if your team has recognised a specific type of attack, it is essential to investigate if the vulnerabilities that allowed them access are still there. Using backups to restore systems to a state prior to an attack may still leave an open door for the attackers.

2. What was stolen/compromised?
   Our investigation will try to identify areas of the organisation that were compromised including systems, data and user accounts. This is useful for communicating with both internal and external stakeholders, and can also be used to place a number on financial impact of the attack for insurance purposes.

3. How did it happen? Who did it?
   Perhaps the initial vulnerability was through a weakness in your defence e.g. un-patched software, or through an attack on a third party supplier with weaker security defences, or through an act of social engineering on one of your employees or even by perpetrated by an employee? By identifying how it happened, we can make sure that measures are put in place so it doesn’t happen again.

4. Can you help me provide information for regulatory or insurance purposes?
   Through a series of interviews and analysis of the forensics we’ve managed to obtain, a report is created to summarise the cyber-attack including details and timeline of both the breach and response. This report will help calculate the financial impact, which can be used for regulatory reports and insurance requirements.

5. How do we make sure we’re better prepared for a cyber-attack?
   Clear lessons have to be identified and learned and demonstrable actions for improvement must be actioned. Of particular importance is your organisation’s strategy for cyber risk management. Is this mature and simply needs tweaking or is significantly lacking and needs better planning. Not all attacks can be prevented, and the increasing number of attacks means that you’re more likely to need to have a well prepared cyber incident response plan (CIRP) and a clear and a well-drilled incident response team (CIRT) who know their roles and can respond immediately when needed.

If you have already been the victim of cyber-attack, Infosec Partners can help you get back up and running confidently, ensuring you are better prepared to deal with the next attack when it happens.

Speak with a trusted advisor today:
+44 845 257 5903
secure@infosecpartners.com

Copyright ©2016 Infosec Partners Ltd. All rights reserved.