What happens when an organisation is attacked?

Are you prepared for if the worst happens?

It is an unfortunate consequence of this technological age that ransomware attacks on organisations can and do happen. In fact, in this year alone we have heard from, and assisted with, multiple clients who have suffered at the hands of a hacker.

To admit to having been hacked by an unknown attacker is often something that organisations are embarrassed to do. As such, we have received communications from clients in which they are evasive about the problem, hunting around with probing questions to try and determine a possible resolution from us without admitting what has happened. Inevitably though, the question is asked “Have you suffered a ransomware attack?”, and once confirmed, we can begin to help where we can.

Attacks have varying levels of severity, something that is influenced by the preparedness of the attacked organisation and the precautions they have already put in place. This does mean that if, as we have witnessed, there are few precautions or little preparedness, an organisation can be in real trouble.

Take backups for example. These are an integral part of getting an organisation up and running again post attack, so what do you do if you find out that you don’t have any backups; where your backups were stored was not safe and these have been corrupted; or your backup process has been faulty and is not functioning properly?

Do you know if your backups are working?

Do you have a system setup within your organisation for regular backups, for example a rolling nightly backup, a monthly back up, and a yearly backup to cover all bases?

- Have you checked that your backup system is working consistently?
- Have you accessed your backups recently so you know that they are viable data and haven’t been corrupted in any way?

Recently, we have witnessed organisations who, after confirming for whatever reason that utilising backups was not possible, had to negotiate with hackers to buy back their data so they could continue to work.
Then comes the rigmarole of workers rebuilding what they can before calling on Professional Advantage consultants to fine tune what they were not able to.

If you do find that you are the victim of an attack and realise that you are going to need assistance with getting back up and running again, don’t delay in reaching out to us for assistance. It will take time to recover from the effects of an attack, so it is important to begin that recovery as soon as possible.
At Professional Advantage, we understand that many organisations don’t want to admit to having suffered from a ransomware attack, fearing both the embarrassment of the situation and the detrimental effect it could have to their reputation if current and potential clients found out. Hence, our priority is simply to focus on and assist you, ensuring you recover.

Now is the time to act!

It is better to protect yourself now than to suffer the consequences of a successful attack later. We have already covered ensuring your backups are working, but what else can you do?

- **Turn on Microsoft 365’s basic security features.**
  Multi-factor authentication (MFA), data loss prevention (DLP), and retention policies are all out of the box security features of Microsoft 365, which means you already have the tools to protect your business data at no extra cost. All you need to do is to turn it on from the Microsoft 365 admin portal.
- **Follow a baseline security model.**
  Microsoft 365’s basic security features combined with proven cybersecurity strategies will increase your chances of mitigating security risks. A typical baseline security model will include common strategies such as Application Whitelisting, Application Patching, OS Patching, Restrictions of Administrative Privileges, Configuration of Office Macros, User Application Hardening, MFA, and Reviewing Backups.
- **Protect your documents wherever they go with Azure Information Protection (AIP).**
  AIP allows you to classify, label, and protect documents and emails based on sensitivity to prevent accidental sharing of confidential information. It encrypts your documents regardless of where it is stored, accessed, or where it ends up.
- **Have regular information security and system reviews.**
  Firewalls and anti-virus software don’t cut it anymore when it comes to cybersecurity. All organisations should perform proactive risk assessments so you can identify the vulnerabilities of your network, server, data, and application. Doing this will allow you to analyse possible threats, determine risks, and set up control mechanisms to decrease your chances of becoming the next ransomware victim.
- **Practice good security hygiene.**
  Using strong passwords and changing them regularly, enabling your staff to identify malicious emails, and boosting your staff’s overall cybersecurity awareness will all contribute towards a more secured IT environment.

If you have any questions or concerns about your organisation's cyber security, or want to know more about what you can do to protect you and or staff, contact your Inside Account Manager.