10 STEPS FOR PROTECTING YOUR COMPANY AGAINST CYBER ATTACKS

BlueVoyant

Knowing about Cybersecurity and putting a number of best practices in place will help you protect your business.

Here are some important best practices that our experts suggest for companies of all sizes.

Secure Corporate Email

Most cyber attacks start with a phishing email, a form of social engineering. Employees are fooled into opening an email and clicking on a link or opening an attachment sent by a malicious actor, which, in many cases is nearly impossible to distinguish from a legitimate sender. This often results in stolen login credentials or a ransomware infection that holds your business hostage unless a ransom is paid.

1. Enable two-factor authentication for all business applications and email - for example using a password and code sent to you by text message. This will most often prevent attackers from logging in by using stolen passwords of your employees.

2. Separate your personal and work email. Attackers conduct their own research on social media and other publicly available websites to make connections between someone's personal life and professional life. Sending yourself emails from your work account to your personal account with sensitive corporate documents or using your work email to register for online accounts exposes you to unnecessary risk.

3. Malware will eventually get through email to your employee's systems. Be prepared to install email protection software that scans attachments and emails for malicious attachments and links. Also, be prepared to install endpoint security software on all of your workstations and servers that only block known virus signatures but will stop malicious behavior like the encryption of files from ransomware.

4. Have someone who understands Cyber Attacker techniques review the alerts that come from your cyber defense software and take action to stop attacks in progress.

Enforce Personnel Policies on "Hygienic" Use of IT

Corporate IT systems generate all kinds of error messages and have operational problems (patches, outages, "bugs," etc). Cyber attackers use this to their advantage: They purposefully design malware to look like "normal" IT operations so that when things go wrong, IT staff, users and even security tools are fooled into thinking its an IT issue vs cyber attack.

5. Provide every employee with a copy of your cybersecurity policy, which must clearly detail what "safe" use of your systems entails, and conduct periodic training on safe cyber practices as well as regular (e.g. monthly) anti-phishing training.

6. Restrict access to sensitive corporate data and files to only those employees who need to know.

7. Make sure that recently dismissed employees have their access to your systems terminated as part of the exit process as soon as possible.

Harden your Corporate Payment Processes

Always assume that compromise of your systems and employee identities can happen. If a cyber attacker compromises an employee with financial access, make sure you have extra controls in place to ensure only valid financial transactions can be made.

8. Do not allow payments to be made to new account addresses without verbal, authenticated confirmation from the responsible party. Relying solely on E-Mail for approval of payment to new accounts without a verbal confirmation exposes you to significant financial losses through common payment redirection schemes.

9. Do not accept internal payment instructions by email that are for any payments other than regular payments - again, verbal confirmation for new or unusual payments by should be part of your process.

Ensure that Critical Data is Backed up and Recoverable

Data is central to your business operations and is very easy and affordable to securely archive - but it won't happen unless you enforce it and test it.

10. Assume that you could be a victim of ransomware, and make sure that the data essential to running your company is backed up and off-line. Most importantly: ***regularly test*** that all your back-ups are working and recoverable.