CYBER SECURITY

Hackers launch an attack every 39 seconds – how vulnerable is your IT system?[1]

18 MARCH 2021

One of the consequences of increased digitalization and connectivity is that it is creating new avenues and opportunities for cyber criminals to hack into IT systems. And as Covid-19 sees more and more people working from home or remotely, more opportunities for cyber criminals are being created. In fact, the FBI's Internet Crime Complaint Center (IC3) has seen the number of reported cyber crimes more than triple since the beginning of the pandemic.[2] In 2021, global cybercrime is expected to cost $6 trillion annually.

At the same time cyber attacks against application programming interfaces (APIs) are also rising, leading to greater adoption of API security measures.[3] According to a recent survey of leading cybersecurity professionals, 91% say they will be making API security a priority in the next two years.[4] However, finding a holistic approach for cyber security remains a challenge.

So, what's the best defence? Here are some of the measures you can take as a first step to ensure your organization is protected.

Conduct an IT security audit

A good starting point is to undertake a full security audit of your organization and its IT systems. This will help identify any vulnerabilities and weaknesses. Remember that all digital interfaces are potential entry points for cyber criminals – emails, websites, apps, cloud storage, connected devices, etc.

Don't assume someone else is taking care of cyber security

One common problem, especially in larger organizations, is that people tend to assume that cyber security is someone's else's responsibility. They take it for granted that it is being taken care of when in actual fact the task has fallen between departments and been overlooked. Cyber security should be seen as a separate function but as an essential part of all business processes.

Make sure all applications are protected

Did you know that 76% mobile applications have insecure data storage which leaves then vulnerable to cyber attack?[5] This exposes sensitive information and 89% of theses vulnerabilities can be exploited without physical access.

Never be complacent

Cyber criminals are continuously probing and searching for IT vulnerabilities and devising new methods for hacking into companies and organizations. You need to be just as vigilant. Always ensure your software protection is up to date, that any new digital interfaces are secure, and that you keep up with all the trends and emerging threats.

Overall, multiple layers of protection are needed, to create a system of protection that encompass all computers, connected devices, networks and software programs. But a strong cyber security system doesn't come down solely on technology and systems – you also need to rely on people in your organization to be informed and making smart cyber defense choices.[6]

The good news?

You don't need to be a cyber security specialist to understand and practice good cyber defense tactics. If you need help to bring your IT systems up to date, reach out to Modis specialists.

Want to learn more? Visit *modis.com*

1 https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds
2 https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic
3 https://www.zdnet.com/article/api-security-becomes-a-top-priority-for-enterprise-players/?&web_view=true
4 https://www.imvision.ai/2021-api-security-survey/
5 https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/
6 https://us.norton.com/internetsecurity-malware-what-is-cybersecurity-what-you-need-to-know.html