Tech Mahindra

Cyberattack

you can be the next!

WHITEPAPER

Connected World.
Connected Experiences.

Overview

It is interesting that most people will agree with this title! At the same time, many companies, from small business owners to global enterprises have no or only inadequate and outdated plans to handle a cyberattack.

Some people believe that if the worst comes to the worst, they will simply bring the "Stake Holders" on the discussion table and sort it out. So on one side, we find them to be pragmatic, while on the other side we find them to be naive - who are "Stake Holders"? What if they are not available?

Not to forget, decisions that are made under emergency & haste are seldom as well thought out, comprehensive and sustainable as decisions would have been made with deliberation in a peaceful time.

Let's define the plan

It is a challenge to draw up contingency and contingency plans for cybersecurity incidents; you don't know what will be the target during the attack and whom will you need, in detail. But there are enough basics that can be well thought and be prepared in advance.

Define what to do in the event of a cyberattack

- Who are the emergency staff?
- At what level of impact/breach and after how long should the attack be reported?
- Who are the people and which are the functions that need to be informed?
- What if personal data has been breached violating the adherence to the data privacy policy?
- Who is responsible for informing customers and employees, who is responsible for handling media, if necessary?
- Who is the contact point with the IT/IT Security service provider, Internet providers and what is the SLA agreed?
- Which competent authority or law enforcement agency can you reach out for help?

Elucidate with your IT department

- **Which services can be switched off, which must continue to run despite the attack?**
  For example, if the mail server was attacked, the web server may continue to run with the website and vice versa.

  If, for example, the server of an essential service of your company has been attacked, a risk assessment must be made. What will cause a lesser impact - power off or try to keep the service running despite attack and defense?

- **How should the cyberattack be contained?**
  Depending on the type of attack, at least the attacking system can be blocked on the firewall. But often that's not enough. In the case of attacks by means of traffic overload such as a DDoS attack, filter mechanisms can be switched on.

- **How can the damage be repaired?**
  The first thing to do is to assess the nature of the impact. For example, in the event of impact from ransomware, importing backups can help. If servers have been encrypted or mail servers compromised, they have to be imaged, analyzed, and rebuilt. In the case of a mail server, the damage to the reputation of various antispam portals must also be cleaned up so that your emails are no longer marked as spam.

- **How do you ensure that your company is free from malware?**
  You need to hunt across your entire IT landscape for the stealthiest malware which may still exist, identify the vulnerabilities which could have been exploited and close them immediately.

- **What can be learned from the attack?**
  It's extremely important to understand the complete attack chain from reconnaissance to execution, effectiveness of BCP, media handling, answering regulators, and more.

- **How can you enhance your cyber defense against the attacks?**
  You may adapt continuous review process and keep revisiting your cyber defense strategy, and tune it in line to the latest threat vectors.

The list of questions can go longer. But the idea here is to provide the first level of a glimpse into why and how you need to be prepared for the cyberattack. Even if you only have a small IT footprint that is operated by an external service provider, it helps to have some details at hand so that you can **act sensibly during a cyber-emergency**.

*We at **TechMahindra** harness the power of strong fundamentals blended with our deep understanding of the ever-changing cyber landscape to prepare, protect and/or rescue our customers from the menace of bad actors.*

Author

Soumak Roy

Global Head, Presales & Solutioning – Cybersecurity, **Tech Mahindra**

Tech Mahindra

www.youtube.com/user/techmahindra09
www.facebook.com/techmahindra
www.twitter.com/tech_mahindra
www.linkedin.com/company/tech-mahindra
www.techmahindra.com
Data&AnalyticsCommunications@techmahindra.com