nccgroup

Shutterstock: Royalty-free stock vector ID: 1349423981

Sep 15, 2020 08:47 BST

With good threat intelligence it's still possible to do security well, even on a tighter budget

Matt Hull, Cyber Threat Intelligence Manager, explains how organisations can get more out of their security budgets by applying good cyber threat intelligence.

Despite signs of recovery in some geographies, organisations around the world are having to carefully review their budgets for the next 12 to 18 months due to the economic impact of COVID-19.

Cyber security is often one of the first areas to be affected by austerity, but it is possible to do security well, even on a tighter budget.

Firstly, organisations should focus on doing the basics properly. Solid fundamentals and good cyber hygiene have always been important, and good estate management, patching, privilege and credential management are all key to getting the most out of a smaller budget. (1)

Secondly, it is crucial to have a good understanding of where threats are coming from. This is where good Cyber Threat Intelligence (CTI) comes into play.

From the Board to the technical staff involved in incident response or security operations, good CTI allows the relevant parties in an organisation to understand the threats that are likely to impact them within the digital landscape.

Armed with this intelligence, organisations can focus their security efforts by basing them on their unique threats and the landscape in which they operate. Ultimately, they can prioritise the allocation of their increasingly limited budgets more effectively.

Good CTI should answer five questions that can be categorised as '5WH's'

Who – *Who is likely to target the organisation?*

This depends on what sector a particular organisation operates in, but you need to know which adversaries are likely to target your organisation. This could range from criminal groups and insiders to hostile nation states.

What – *What are they looking to target?*

Identifying critical systems, key personnel, and important data assets such as customer data or intellectual property will allow an organisation to assess the risk of these assets being targeted.

Why – *Why are they attacking you or likely to target you in the future?*

Understanding the motivations of malicious actors means that an organisation can prioritise defences for the systems or data that are likely to be targeted. For example; a criminal group which is primarily financially motivated will be more likely to target payment processing systems.

Where – *Where is the attack likely to come from and where is it going to have an impact?*

Where a cyber-attack comes from can often be influenced by geo-political factors. Where an organisation is based, or operated from, could be reasons for it to be targeted.

When – *When is the organisation going to be targeted?*

Identifying the possible future trends in threat actor activity by horizon scanning allows an organisation to plan strategic and operational responses well in advance. Having an understanding of new technologies, geo-politics, and even seasonal changes in criminal activity is key to identifying future threats.

The '5WH's' will also be able to answer the final question on how the attack will happen:

How – H*ow is the attack likely to happen?*

Having assessed the "who, what, why, where and when", it is possible to assess probable attack vectors that could impact the organisation. This includes detailed technical information with regards to Tools, Techniques, and Procedures (TTPs) of threat actors based on evidence of their previous activities.

Only through good CTI can organisations fully understand the risks that that they face day-to-day and year on year. By understanding these things, organisations can gain a more informed view on both resource allocation and appropriate defensive actions, and ultimately use their security budgets more effectively.

[1]https://newsroom.nccgroup.com/blog_posts/risk-vs-cost-cyber-in-the-face-of-economic-uncertainty-94626?utm_source=rss&utm_medium=rss&utm_campaign=Subscription&utm_content=current_news

---

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and

innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970