Majority of companies not confident about ‘business as usual’ 24 hours after a cybersecurity incident – NTT Security poll

Submitted by: Origin Comms Ltd
Thursday, 21 March 2019

The clock starts ticking immediately following a cybersecurity incident with the first 24 hours vital in terms of incident response. According to a new social media poll (https://www.nttsecurity.com/docs/librariesprovider3/resources/uk_infographic_ir-poll_uea.pdf?sfvrsn=79325d7_6) by NTT Security (https://www.nttsecurity.com/en-uk), the specialised security company and centre of excellence in security for NTT Group, the majority (59 per cent) of respondents admit they are not confident their company could resume ‘business as usual’ after the first 24 hours, although 41 per cent say they are.

Asked about their number one focus in the first 24 hours after a security incident, nearly two-thirds (64 per cent) of respondents say mitigating the threat is the main priority, while 36 per cent say it is about identifying the cause. David Gray, Senior Manager and Incident Response Practice Lead EMEA at NTT Security, believes that although there is much greater security awareness from top to bottom within organisations, there is a clear lack of preparation and planning when it comes to incidents, despite the potential impact.

“There is still an element of ‘head in the sand’, where organisations simply don’t think it is going to happen to them, despite everything we are seeing in the news. Our global Risk:Value (https://www.nttsecurity.com/en-uk/landing-pages/risk-value-2018) report* last year backs this up, with less than half (49 per cent) of respondents admitting they have implemented an incident response plan. While most say they communicate their plans internally, it’s still only a minority who are fully aware of them. These figures have barely changed year on year and suggest that incident response planning is still not a priority.”

The NTT Security poll, which was conducted over Twitter and generated around 5,500 responses, points to a lack of resources that many organisations are struggling with today as a possible explanation for this. Lack of skills in-house is what worries the majority of companies (59 per cent) when responding to a cybersecurity incident or breach, while 41 per cent worry about lack of budget.

David Gray adds: “The worry is that even if organisations do have an incident response plan in place they simply do not have the resources to execute it, losing valuable hours or even days identifying the right skills and setting up the necessary SLAs and contracts. This is precious time wasted. Even the most mature security teams are forced into a reactive stance when something happens. Those first 24 hours are crucial in minimising the impact and cost of an incident and protecting valuable data, so they need to make them count!”

Steps to take in the first 24 hours of a security incident

NTT Security recommends adopting a triage process in the first 24 hours of a security incident to provide a head start in remediation and post-incident investigation. These steps provide a starting point to this process:

Detection
Understanding how and when an incident was first detected is the best place to begin. It may be some time since the systems were compromised, but asking questions, such as whether firewall logs are being used to their full potential to identify the initial compromise or if there are other SIEM solutions in place could help to uncover vital clues.

System framework
In order to provide an effective response you must know where the servers and/or endpoints are physically located. Equally important is the setup, i.e. operating systems, storage, virtualisation as well as security configuration, i.e. user groups/permissions as well as a network map.

Preliminary remediation
Providing accurate handover notes to an incident response team along with a record of the steps taken up until that point are recommended in order to prevent any cross-contamination or incorrect leads being pursued. To ensure IT, CISO and incident response single point of contacts are fully engaged with one another it is essential that this communication is continued throughout the course of the incident response plan.

Logs provide crucial evidence
Log files may be crucial in uncovering and identifying indicators of compromise (IoC) or detecting the intrusion. To avoid mislaying any evidence, logging must be fully enabled and retention periods applied and provided at the earliest opportunity to ensure a thorough review to determine IoCs.

Artefact preservation
The preservation of artefacts identified within data must be maintained to carry out comprehensive forensic analysis and so that an accurate timeline can be constructed. Each incident must be treated on an individual basis and this process should be employed whether or not external authorities are engaged. If they are involved then the reports could form key evidence.

For more information on NTT Security's Incident Response and Remediation solutions visit: Incident Response retainer services (https://www.nttsecurity.com/en-uk/landing-pages/incident-response-retainer-services)

Additional information

Infographic
(https://www.nttsecurity.com/docs/librariesprovider3/resources/uk_infographic_ir-poll_uea.pdf?sfvrsn=79325d7_6)

* NTT Security 2018 Risk:Value report: Risk Value 2018: https://www.nttsecurity.com/en-uk/landing-pages/risk-value-2018

About NTT Security
NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for

clients' digital transformation needs. NTT Security has multiple SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html

Amanda Hassall, Consultant, Origin Comms
amanda@origincomms.com
M: +44 (0) 78 5535 9889
T: +44 (0) 16 2882 2741