Managing the supply risk in your supply chain

What is the problem?

Traditionally, organisations have focused their cyber security effort and budget on ensuring that their own environment is as secure as possible. From ransomware protection to encryption, companies have locked down their data to protect their crown jewels: their data.

We have seen from the multiple breaches declared recently for clients of SolarWinds or MoveIT, to name just two, that managing the risk in your supply chain now takes on a more significant requirement; in addition to the risk from close supplier interaction, it is no longer possible to point the finger at your supplier as there is a joint responsibility for any breach. With new legislation for the Digital Operational Resiliency Act (DORA) or Network Infrastructure Security (NIS) regulations, supply chain security is a key pillar of your Cyber Resilience programme.

What is the standard process now?

Under recent GDPR legislation, the scope for data security was broadened to incorporate your suppliers to ensure that companies have a more rounded approach to protecting their data. Some underwent extensive programmes to work with their suppliers in a joint process, but most resorted to a more basic approach: a bespoke questionnaire was created, passed to suppliers to complete and then checked (or, often, not) and filed away for a year or two. If you trawled through your suppliers' responses, the chances are that everyone declared themselves secure, with no outstanding issues to be resolved.

How can you build a real-time monitoring solution?

So, how do you independently monitor your supply chain and make business decisions based on the risks highlighted by your findings? It is no longer acceptable to ask for your suppliers to mark their own homework, so what can you do to assess what potential risks you face?

We have an inexpensive solution that provides you with the same viewpoint that a potential hacker would have when looking at both your domain and that of your key suppliers.

How do you create a hacker's view of your supply chain cyber risk?

All of the data we assess is in the public domain, so there is no port sniffing, no software to be installed and no interruption of your supply chain network. We find, assess and report back on such issues as:

- Known patching vulnerabilities
- Open ports
- SSL certificate mismatch or expiry DNS issues
- Domain variants
- Leaked passwords

  and much more

Initially, we run this service across your domains, after which you can extend the service and run the reports against your key suppliers.

We report the findings to you in a regular meeting, using the live data and our technical specialists to recommend remediations.

This service covers:

- A monthly, full-featured Cyber Profiler report containing our findings and observations. And insights to inform your defence against cyber-attacks.
- Using the report, a monthly guided specialist review by a named contact discusses all known vulnerabilities {CVEs), certificate issues, breached email addresses, domain issues and internet-resolvable hosts identifying addressable vulnerabilities. The designated contact will agree on a course of action for each identified vulnerability.
- Access to consultants who can help assess reconfiguration options for the attack surface.
- Scheduled remedial activity and consultant activity to address known vulnerabilities and, where possible, attack surface reconfiguration.
- Recommendations for supply chain issues where necessary

As always, data security is not a one-off or annual occurrence like a traditional pen test. Maintaining regular reporting allows new issues to be covered without waiting until the annual report is produced. It also allows you to track your suppliers to ensure that they maintain their cyber resilience from week to week.

With cost control always under review, we can offer a managed cyber-service across a domain from as little as £10,000 + VAT per year. It's the same as an annual pen test but with 24 x 7 x 365 reporting.

Contact us for more information, call 0207 4488500 or email info@northdoor.co.uk or visit www.northdoor.co.uk

northdoor
Store IT · Protect IT · Use IT