Vulnerability Management

6 Challenges Seen by Our Cyber Security Team

TECHNOLOGY SOLUTIONS

Cyber security solutions are abundant in the current marketplace, from enterprise options like Tenable, Rapid7, and Qualys to open-source tools like OpenVAS or free 'add-ons' to AV and EDR tools. The area traditionally known as Vulnerability Management in some cases is even referred to now as Attack Surface or Exposure Management. What you need to remember is that despite the advanced metrics, dashboards and artificial intelligence, the human element remains key for configuring, interpreting, and acting on results.

PATCHING

Patch Management, the bain of most IT teams lives but an imperative in having an effective solution in place. End users complaining about interruptions and loss of productivity, IT having to conduct testing before rolling out patches 'en masse' to circumvent potential operational issues, are but a few of the difficulties, challenges and time constraints that are faced by the human element. In addition to this, third party patches are overlooked with the most effort being put into Microsoft infrastructure and applications. We also see poorly configured patch management technology on many occasions, and on others, a 'capable' and 'comprehensive' patching solution is missing.

PENETRATION TESTING

Nobody wants to make a penetration tester's life easy, however discovery of easily exploitable vulnerabilities across multiple devices will do just that. The harsh reality is that most pen testers will volunteer this is the case and that little improvement is seen from year to year; same scope, different vulnerabilities. It is commonplace for vulnerabilities discovered during a pen test exercise to be prioritised for remediation, which would be great, were these not replaced by new ones the moment the pen tester completes the engagement.

EFFORT LEVELS

Effort levels and the focus of attention are undoubtedly heightened following a penetration test or when preparing for a Cyber Essentials Plus audit. During these times, organisations often allocate additional resources, increase vigilance, and prioritise cyber security measures to ensure compliance and address any vulnerabilities that may have been identified. However, it is crucial to recognise that this elevated level of effort and scrutiny should not be a temporary measure, confined only to these specific periods.

TIME, RESOURCE AND EXPERTISE

Maintaining a consistent and proactive approach to vulnerability management is crucial for ensuring the security of your systems and data. However, this can be challenging due to limited time, resources, and expertise. Key challenges include the time-consuming nature of vulnerability scanning, assessment, and mitigation, the need for specialised tools and personnel, and the evolving threat landscape. To address these challenges, organisations should prioritise vulnerabilities based on risk, automate where possible and regularly assess the effectiveness of their processes with set goals in mind.

VISIBILITY AND COMPLACENCY

Lack of visibility of current vulnerabilities, misconfigurations and context of what to tackle first will inevitably make life impossible. Whether that's through lack of a comprehensive solution that doesn't have the ability to refresh up to date vulnerabilities automatically, or potentially poor engagement levels or understanding of the over complicated solution in situ. We have seen organisations firmly believing they are in control of vulnerabilities because they patch on a regular basis, but without a tool to provide that 'source of truth', this on most occasions is unfounded.

PLANNING FOR SUCCESS

Planning and management on an ongoing basis is key to success. We have seen some amazing results from a number of customers who have made this area one of their monthly focal points, discussing metrics, successes, ongoing issues, requirements for additional investment from the business and along the way uncovering team members who have taken a keen interest in improvements and general security hygiene.

DATACONNECT
CYBER SECURITY - CONSULTANCY | SERVICES | TECHNOLOGY