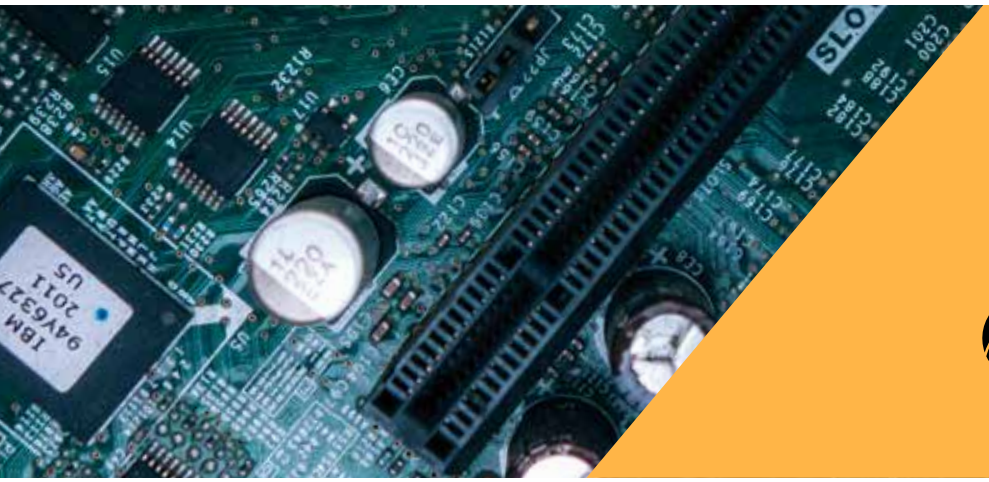

OSIRIUM

Separate your business from cyber-attacks

OSIRIUM REPORTS

The cybersecurity landscape is ever changing. New threats appear daily, and the techniques used by attackers continuously evolve.

2017 bought us the biggest ransomware outbreak in history in the form of WannaCry, and an Equifax data breach that exposed the personal information of nearly half the United States' population. 2018, following trend, started with the disclosure of the Meltdown and Spectre vulnerabilities, which put practically every operating system and device on the planet at risk.

With the rate of attacks constant, it can be difficult to keep up, even for the most seasoned cybersecurity specialist. In this blog we map out the threat landscape for 2018, and give you advice on how best to separate your business from risk.

Who executes cyber-attacks?

Verizon's 2018 Data Breach Investigations Report identified over 53,000 attempted and 2,216 confirmed cybersecurity exposures over the course of 2017. External threat actors continue to be behind the majority (73%) of cyber attacks, consisting mostly of organised criminals, but more pressing is that internal actors account for 28% of incidents and breaches.

Almost 3 in 10 cyber attacks are executed by trusted insiders, with System Administrators being identified as the biggest threat, behind 25% of confirmed breaches. These privileged users require elevated control through privileged accounts to ensure the uptime, performance and security of the entire IT infrastructure. Unfortunately, privileged accounts are increasingly a hacker's favourite target, and privilege account abuse presents one of today's most critical security challenges. Uncontrolled access to privileged accounts effectively provides rogue insiders or external hackers with the keys to the kingdom.

How and what is stolen?

The two main tactics utilized by cybercriminals during 2017 were hacking (48%) and malware (30%). Phishing individuals and installing keyloggers to steal credentials was a common path. The use of stolen credentials (22%) was top of the charts in successful breaches, followed by RAM scraping (17%), phishing (13%) and privilege misuse (11%). Databases were the main assets stolen, made up of 38% personal data, 28% payment data, 25% medical data, and 11% credentials

How can you prevent becoming a victim? By separating people from passwords!

To counter cybersecurity attacks, we advocate separating people from passwords (or to be exact: separating SysAdmins from privileged credentials).

cont. overleaf

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password lifecycle management, and then hand the pre-prepared session back to the incoming request ready for system management. The session can be recorded, subject to time windows and device group separation. We have delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.

"The use of stolen credentials was top of the charts in successful breaches"

Osirium's Privileged Access Management solution, the PxM Platform, helps to reduce risk by separating privileged users from privileged credentials. It does this by acting as a proxy connection between the user and the device. Users simply identify themselves to the PxM Platform and receive a list of assigned devices, applications, tasks and roles. On each choice, the PxM Platform performs the single sign-on or initiates the task. Privileges are restricted to what users need to do the job, and credentials are never revealed. As privileged credentials never cross into the domain of the users' system, they cannot be stolen, misused or phished.

In addition, the Privileged Session Management module of the PxM Platform provides further protection by allowing IT managers to record, store and playback any activities that take place across their entire hybrid-cloud infrastructures. This acts as a deterrent for internal privilege abuse. The Privileged Behaviour Management module of the Osirium PxM Platform reduces detection time by using machine learning techniques to create a baseline of expected activity for each privileged user. Active threats can be identified quickly from anomalous behaviour, and passive threats can be identified in users that have high privileged roles assigned that are not being used (also known as privilege creep).

Driving towards overall compliance and security

Furthermore, the PxM Platform helps companies meet increasingly stringent compliance standards such as ISO 27001, Cyber Essentials, PCI DSS, MAS TRM, NIST 800-53 and GDPR, minimising both the risk of a breach and its' potential economic sanction.

By understanding what data types are likely targets and the application controls that make it difficult to steal them, businesses can set about thoughtfully and intelligently protecting themselves. Whilst there is little guarantee of total safety, the PxM Platform allows businesses to proactively protect what is most valuable – their privileged credentials – by separating people from passwords and making interception an impossibility.

If you'd like to find out more about the PxM Platform, please get in touch.