Maintaining PAM in the legal industry

OSIRIUM REPORTS

Privileged (i.e. administrator, system, root) Accounts are the gateway to your confidential data. Compromise and misuse of their credentials (Username, Password/Token) accounts for 99.8% of all data breaches. The remainder are mostly caused by data being left unprotected or accidental mis-forwarding.

The dark net has become a simple truth of online life. This underside of the internet used to be mostly indiscriminate: malware would be created and the perpetrators would sit back and wait to see who they caught. These days over 90% of malware is directed at individuals or organisations. Untraceable payment technologies have led to a burgeoning market in 'hackers for hire'.

In simplistic terms, malware falls into two categories: a) Those that deny service and hold the victims to ransom; and b) Those that seek to extract privileged credentials in the most stealthy way possible.

The overall statistics (Source: Verizon Data Breach Investigation Reports) show that 86% of all passwords are stolen at the desktop, 10–11% are phished by social engineering and the remaining 3–4% are brute forced. Of interest is that brute force is beginning to rise again because complex password policies are actually counter productive.

Outsourcing has become a common attack vector. In the huge attack on Target in the US, the goal was to access customer payment card details.

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.

Target's own digital hygiene was in reasonable shape, so the attackers focused on an air-conditioning contractor that had virtual network access in order to monitor the installations at Target's head office.

Law firms are all about trust and confidential dealings. The internal IT teams will be tasked with protecting the firm from cyber attack. Ironically whilst they are protecting the firm they are the most likely to be targets for attack. Furthermore, they have the most passwords to remember and are the most likely to share their passwords with colleagues.

At Osirium, we've learned that people are far less likely to share their identity than share credentials. That was the driving force in creating a product that separated people from passwords whilst making the SysAdmin's life easier and more productive.

We take the approach of 'identity in role out', this means that a SysAdmin (or outsourcer, supplier, contractor) presents their identity and Osirium's PxM Platform makes the connection and authentication to the system for them. Therefore the PxM Platform is managing the password-device relationship. This means that the PxM Platform can use 128 character, truly random passwords and then cycle these on a scheduled basis – the SysAdmin is never burdened with the need to remember multiple huge passwords.

This works well with shared accounts, for example root, and domain admin. As a legal aside it means that no-one can use the so called 'root defence' whereby the accused can argue you can't prove it was them because everyone else in the department knew the root account password. It's easy to see how this would be a powerful deterrent to any insider wrong doing.

There are many common tasks in the IT world that need high privilege or responsibility; for example, setting and reseting passwords, queue purging and the like. These tasks get delegated to the help desk to meet the 'first call fix' SLA. The PxM Platofm's task engine means that these can be wrapped into pre-packaged, parameterised GUI based operations. Now no-one in the Help Desk team need ever be issued with a domain admin password again.