OSIRIUM

Controlling the outsourced outsourcer

OSIRIUM REPORTS

Provocative title, but here's how it happens: your organisation outsources the management of some servers and workstations. That outsource company then outsources the management of the anti-malware components to a specialist outsourcer. They, in turn, outsource the repetitive tasks to the cheapest labour source they can find.

Your organisation could be lucky, they could have chosen a managed service provider who uses the principle of 'identity in – role out'. For example, they may use a specialist company to manage large scale anti-malware deployments. These two companies would work together so that they can see who did what, where, and when. This builds fundamental trust between the two outsourcers which translates to better business for the MSP's customers.

Working with outsourcing generally means that you are expected to hand over the credentials to a set of privileged accounts on your systems. These are then built in to 'run-books' that the outsourced SysAdmins use to ensure that they deal with your systems in a consistent way. This is a problem: they need to carefully control who can see those run-books, and they need to trust that the run-books they outsource themselves are treated with respect.

If you've ever been to an offshore call centre you'll know how busy and chaotic they seem. Look around, take note of the age of the desktops and versions of the OS they are running. If you look closer it's more organised than

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.

it seems, but often organised on a friends and family basis. Our support account is full of questions about deployments in Company A from someone in Company B; when we bat these back we'll get a whole host of replies along the lines of "My brother's English is not so good" to "I used to work there". It's clear that there is a case of what the contract states and what actually gets done!

The first part of the solution is to separate the people from the passwords used on systems, devices and applications – never allow the passwords to enter the SysAdmin's domain. This stops the diffuse proliferation of privileged credentials, and removes the possibility of them getting intercepted or RAM scraped. Completing this stage means that you'll no longer need to share passwords to admin, root and maintenance accounts. Using Enterprise Class Password Lifecycle Management means that all passwords will be long, strong and regularly changed.

The next stage is to verify the identity of the people wanting to connect to your systems.This identity needs to be mapped onto a profile of the roles on systems they should be allowed to use. With the user's identity confirmed, connections can be established for the user using Single Sign On, ensuring that the SysAdmin never has to know any credentials.

People will protect their personal identities far more than they'll protect a set of credentials from an organisation. Two factor authentication takes this a stage further. It makes sharing identity more difficult since both parties would need access to the token.

To complete the control you need to make it clear that you'll record all sessions that third parties have with your systems. This is the ultimate deterrent for those that don't want to be caught and the ultimate forensics resource for reversing wrong doings.