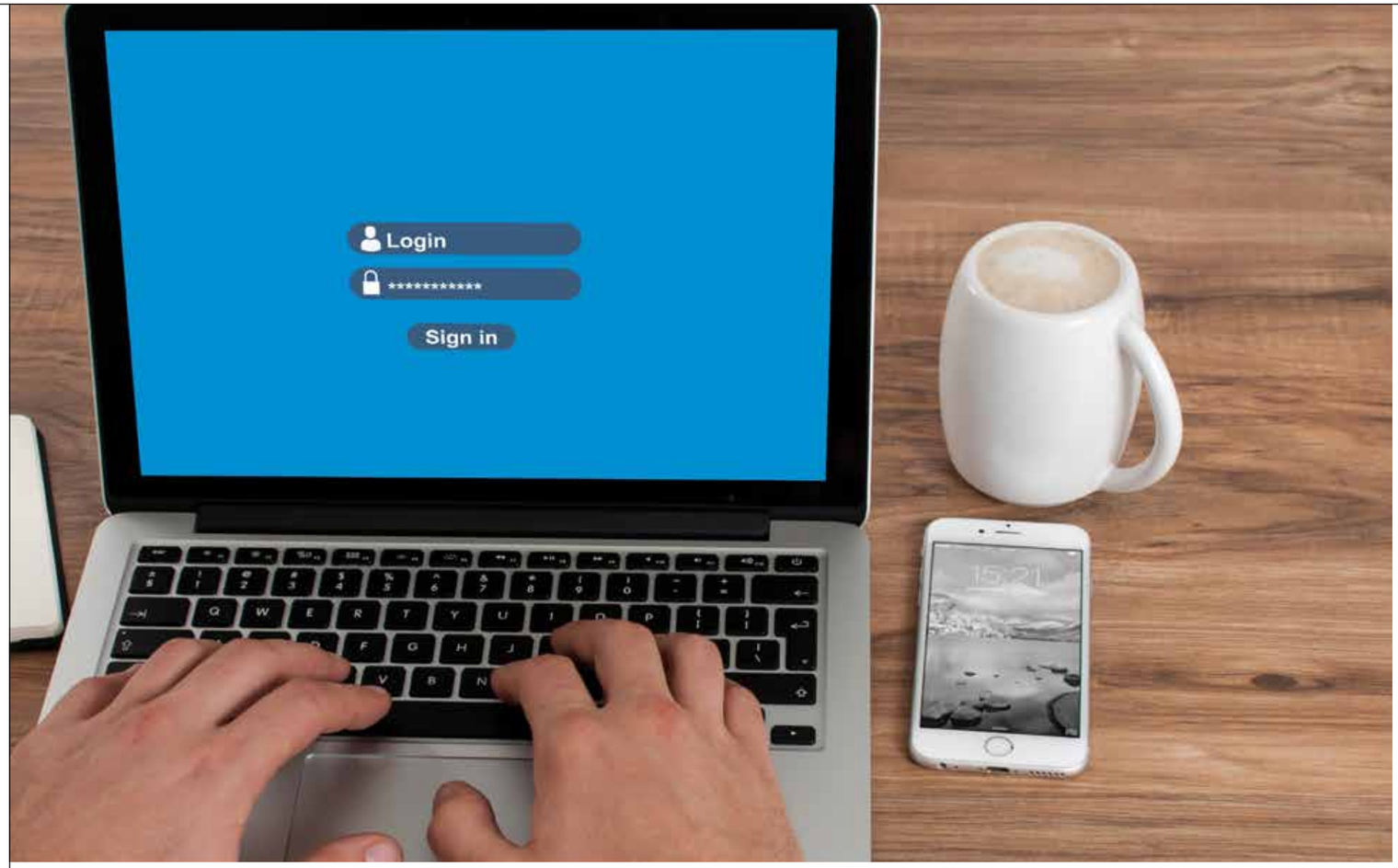

IDENTIFY YOURSELF

Joseph Carson *reveals why organisations need to embrace identity as the future perimeter*

The world of work has long been a place as much as a function. Technical limitations meant that workers needed to be onsite to access resources. Even as technology advanced, tradition held. Consequently, network security has historically been concentrated on specific workplaces too, with most strategies relying on a static, secure perimeter at the location.

And then came COVID. The pandemic not only opened the door to the possibility of remote working, it forced organisations through it, whether they were ready or not. It accelerated business transformation and the adoption of remote working.

Two years down the line, with normality resuming, the door to remote working remains open. While most organisations have returned to office-based work, a significant amount have retained some level of flexibility. The ONS found that between 16 and 27 February 2022, 15 percent of UK employees worked from home because of COVID. In this hybrid working world, in which the boundaries have shifted, identity is the new perimeter.

Relying on legacy security to protect the network layer, while also enabling remote workers and making use of cloud-based assets presents a number of problems. For example, the strategy might rely on the presence of enterprise-grade secure routers, while workers at home will almost certainly be using commercial routers that cannot offer the same level of protection – typically with default credentials. But it is not feasible to equip potentially thousands of individuals with a router for each location, nor to mandate that they purchase one themselves.

The biggest issue with a legacy perimeter-based approach to security is the way in which it handles identity

Similarly, cloud-based assets and infrastructure will not benefit from any location-based perimeter security, rendering these legacy solutions increasingly moot as cloud migration continues. We have started to shift from BYOD (Bring your own Device) to BYOO (Bring your own office) and employees' homes are almost becoming mini cloud sites where the employee operates from.

The biggest issue with a legacy perimeter-based approach to security is the way it handles identity. The standard username/password combination has been the staple of user identity for many years, and organisations still have critical assets that can be accessed without any further security controls or verification.

Threat actors are well aware of this and the majority of attacks concentrate on exploiting this critical weakness. The 2021 Verizon Data Breach Investigations Report found that 61 percent of all breaches were the result of attackers exploiting data through leaked or stolen credentials, or via brute force and credential stuffing attacks. The report also highlighted a continued increase in phishing attacks as adversaries attempt to trick targets into sharing their credentials by impersonating colleagues, IT personnel and systems themselves.

However, criminals often don't even need to go to the effort of creating a social engineering campaign. Weak, manually, human-generated passwords can be quickly guessed by automated brute force attacks. The tendency to re-use the same passwords in multiple places also opens the threat of credential stuffing attacks that attempt to use credentials stolen in previous breaches.

Once an attacker has a working set of credentials they will be able to walk right in unless the organisation has other layers of identity security in place. The effect is a locked portcullis that can be opened by anyone who finds, steals or duplicates a key – and there happens to be thousands of copies around.

Once an attacker is inside, research indicates that the average dwell time stands at 24 days – ample time to exfiltrate data, plant targeted malware, and establish back doors. It also provides the opportunity for more organised threat actors to expand their attack into the supply chain.

Privileged accounts with elevated levels of system access and admin power are the ultimate target of most cyber attacks. Accounts such as local and domain admins have a large array of capabilities that can be exploited. Threat actors can use Active Directory to create more accounts with increased authorisation, access and edit critical data and systems, and change logs to hide their tracks.

Nevertheless, we often find accounts are poorly managed. Many enterprises still have privileged accounts governed by weak passwords open to brute forcing and credential stuffing. Privileged account creds are also frequently saved in unencrypted Excel or text files, and freely traded across email and channels like Teams and Slack. This means that compromising a single standard user can quickly grant access to powerful superuser abilities.

Another common mistake is to focus on employees and overlook non-human users. Modern IT infrastructure relies on service accounts to provide access for automated systems, which often have a high level of privilege. While most workers will not even be aware they exist, they can be exploited by threat actors in the same way as human-facing admin accounts.

Identity is now the focal point for cyber-attacks and so it should be the main security control. User accounts should be thought of not as simple combinations of usernames and passwords, but as trusted digital identities tied to specific individuals and their specific roles.

The Zero Trust framework has emerged as one of the most effective ways of managing this. Simply having a set of credentials is the first step – users must also prove they are trustworthy before they can access anything on the network. How this is earned will vary depending on the situation, with a risk-based process accounting for the importance of the assets requested, as well as factors such as the user's location and endpoint device they are using.

A user sitting at their desk from their recognised machine will be given relatively easy access, while someone using an unfamiliar machine in an unusual location will need to jump through a few more hoops to confirm they aren't an imposter. It will act like a digital polygraph test asking the right questions to confirm the identity is authentic.

MULTIPLE LEVELS OF SECURITY HELPS VERIFY THE USER IS REALLY WHO THEY ARE CLAIMING TO BE

When it comes to special privileged accounts shared by multiple users, a rigid adherence to least privilege is required, ensuring that accounts and systems can only be accessed as part of core job functions. A Privilege Access Management (PAM) solution is also important to keep credentials safe and keep track of how these accounts are being accessed and used.

Identity should be separated into two elements. First is verification, confirming that the user is who they claim to be. Second is authorisation, governing what they are allowed to do once their identity is confirmed. A modern equivalent could be a well-guarded bank, complete with vault and safe deposit boxes. Getting into the building itself is accomplished with a mere visual check from the guard, which will provide a bare minimum of security, keeping out known undesirables. Accessing the safe deposit room, however, requires another level of authentication to prove the visitor has the right to be there, such as further ID or the use of biometrics. Finally, actually opening the safe box requires the use of a key, while also under the watchful eye of a security guard.

In this convenient example, the contents of the safe deposit box are protected by multiple layers of security to authenticate the visitor's identity and authorise them to access the box. However, this also creates a cumbersome process for legitimate customers to go through. This is bearable for occasional visits, but quickly creates friction if it must be repeated on a regular basis. In a digital setting, users will need to verify their identities several times every day as they navigate the system and access restricted data and applications. Having to jump through hoops every time creates a negative user experience that can also start impacting productivity. Security must be balanced against usability.

The answer to this problem is to establish a pyramid of controls that allow users to move laterally based on

the level of trust they have earned. So going through the lowest level of authentication using credentials, allows access to only low-security areas of the network. Attempting to access something more secure requires additional authentication through multifactor authentication (MFA) or a VPN. Once this has been completed, the user is free to access other applications at the same security level without authenticating again unless the risks change or time has expired.

ONCE AN ATTACKER IS INSIDE, RESEARCH INDICATES AVERAGE DWELL TIME IS 24 DAYS

Attempting to move up again, let's say accessing AD to create a new user account, requires the strongest form of authentication, such as a more strict form of MFA or authorisation from a colleague. Authorising at this level means the user is free to access anything further down the pyramid for the rest of the session.

For an excellent example of this process at work, one can look to the Estonian government, which has launched a raft of digital services in recent years. Once a user has signed into the service portal using their government ID as the trust anchor, they can move laterally to access multiple different provisions such as renewing their driver's license or updating their personal details. The process provides an efficient and frictionless experience for users without compromising on security. Having multiple levels of security from authentication to digital signatures, helps verify the user is really who they are claiming to be.

Moving towards identity-based security can be a significant task, and many enterprises are still stuck with security strategies geared to an outward-facing perimeter around their network. A combination of limited budgets and the baggage of years of legacy infrastructure and technical debt can make it difficult to make the jump, even as firms also pursue cloud and remote working.

However, an identity-based model and Zero Trust approach do not have to be accomplished in a single bound. Enterprises should look at small-use cases in the first instance to get a feel for the process and prove the value of the approach, and then gradually spread out to other parts of their operations. Critical systems and privileged accounts that pose the greatest risk should be the priority here.

LAYERED DEFENCE

An important initial step is to evaluate the current IT and security stack and scope out areas that can be better integrated. The ultimate aim is to create a single, centralised control point that can manage identity across the entire infrastructure. Future investments should be centred on interoperability – creating a layered defence of solutions that can work together.

A highly integrated stack will also make it easier to implement automation – the second priority. Authentication, authorisation, monitoring and all other secure access processes should be guided by automated policies that can apply adaptable risk-based rules and create a frictionless user experience.

The third priority is orchestration. Everything should work together seamlessly, with no gaps or blind spots that could be exploited by threat actors. PAM tools are useful here as they can help the security team manage and secure credentials across the entire organisation, for example removing the risk of manually created passwords waiting to be discovered in text documents.

Traditional, static perimeters can only guard against the threats of the past and are easily bypassed by today's threat actors. Establishing identity as the new perimeter, supported by a frictionless authentication system, will enable organisations to continue adapting to the latest working developments without leaving the door open for threat actors ●

Joseph Carson is Chief Security Scientist and Advisory CISO at Delinea

The tendency to re-use passwords in multiple places opens up the threat of attacks