ManageEngine
PAM360

The importance of privileged access management in digital transformation

Erin Casteel

www.manageengine.com/pam360

Digital transformation is a ubiquitous, loaded term that is increasingly used to describe or justify just about any IT project. However, digital transformation and evolution is not optional or discretionary—it is essential today for every organization, from small businesses attempting to compete with larger enterprises, to industry stalwarts trying not to become irrelevant by innovative and agile up-and-comers.

Digital transformation initiatives can make it possible for an organization to accomplish more in less time with less cost, and allow it to continually adapt to the ever-evolving needs of customers, staff, and other stakeholders. However, to be successful, cybersecurity needs to be embedded in all digital initiatives from the outset—not as an afterthought to be bolted on later. This can sometimes be a challenge; it requires different groups with disparate expertise and contexts to have an understanding of cyber risk, and to work together with a common vision.

Where to start

To understand the benefits and risks of digital transformation and its relationship to cybersecurity, it is crucial for everyone to start on the same page, including business and IT leaders, cybersecurity teams, developers, cloud engineers, and partners. Digital technologies and projects can provide opportunities to dramatically improve operational excellence as well as deliver new product offerings, competitive advantages, and increase velocity and agility. Digital transformation initiatives are designed to help us share data across different systems and platforms easily. But with increased efficiency and productivity, comes the potential for greater complexity and increased risk. Each new technology and step along the digital journey has the potential to increase cyber risk by multiplying the organization's attack surface, increasing complexity, and exposing more assets to the internet.

It is imperative for organizations to ensure that their digital transformation initiatives are planned and implemented from the outset with "security by design". Since the beginning of the pandemic in early 2020, we have seen exponential digital growth. During this time, many organizations across multiple industry sectors have also matured in their understanding of cybersecurity and cyber risk. Evolving from the binary concept of "we are either secure or not" to a holistic understanding of cyber risk, our IT security focus needs to be on cyber resilience rather than a strategy solely based on elimination of threats.

Business and IT leaders increasingly understand that in today's environment, traditionally siloed or "fortress" approaches to cybersecurity are no longer viable. The modern network does not have clear boundaries, and functionality is more and more dependent on connectivity. There is no such thing as a completely secure, connected system. This is why constraints, like limiting access privileges, are so important. Once a cybersecurity breach occurs and access to one system has been achieved, without the right controls to protect access to each system or data repository relevant to the organization, an attacker can move much more quickly through an organization's whole network.

Privileged access management

What is needed is an agile, multi-layered approach to cybersecurity. A core requirement is a privileged access management (PAM) solution that is integrated with a robust, well-controlled PAM practice encompassing people, processes, policies, and the organization's ecosystem as well as its technology.

PAM helps manage accounts that have access to confidential, high value, or business-sensitive information, or the ability to make admin level changes. PAM protects the organization's information, identities, and systems

through privileged accounts monitoring, preventing internal and external threats that result from the improper use of data or admin rights. With the principle of least privilege at its core, PAM solutions emphasize giving the minimal access required for users to complete their activities or responsibilities.

PAM is fundamental to achieving a more secure digital transformation. Privileged access control includes access rights not only for users, but also for devices and applications as well as automated processes. It is vital to have clarity about what access each identity (human or otherwise) requires to what systems or data, and how that system or data will be used. It is also important to validate whether an identity is who or what they are supposed to be, to track any changes to identities or requirements, and to ensure that these changes are managed in a timely and secure way.

In operational terms, this means that every connection needs to be authenticated and every activity authorized, based on the roles and permissions established according to the organization under the principle of assigning the least privileged permissions to each entity for the least duration of time possible. This facilitates the traceability of access to information and assets, and reduces gaps in visibility and control.

It is essential to consider that non-human privileged accounts can easily be neglected and forgotten if they are not being actively monitored and managed through PAM. A breach of these types of privileged accounts has the potential to remain undetected for a longer period, with severe consequences if the right controls are not in place.

Why PAM is the priority

At least 80% of breaches involve compromised privileged credentials[1]. From a cyberattacker's perspective, obtaining privileged access information has the highest value (including the highest ROI) of any attack strategy.

While identity and access management is a related practice used to manage every user account in an organization, PAM is focused on securing access to higher value (representing higher risk) business and technical system accounts. PAM protects access to the accounts which, if breached, would be the most devastating. This means PAM should be the priority for organizations when they consider which IT security capabilities to put in place first.

PAM can automate the provisioning process for privileged accounts, which can increase efficiency while also ensuring consistency and compliance, reducing the need for constant manual verification and intervention. This is particularly relevant to digital transformation initiatives, which can benefit from the reduced cost and risk, and increased efficiency of automation.

A change of mindset

With the traditional, siloed or "fortress" approach to cybersecurity, there was once an idea that it was possible to keep threat actors outside the firewall and that everything inside the firewall was, by default, "safe". Today, we try to imagine that the attacker is already inside—already in your workstation and waiting for you to do something to exploit—rather than only a potential threat. We are even hearing more and more about threat actors trying to recruit corporate insiders to help them breach networks. In return, the insider is promised millions of dollars.

Managing cyber risk today is about limiting what an attacker can see and do rather than assuming it is possible to keep them out. Identity, access, and particularly privileged access management have become the new perimeter, the new firewall.

As organizations are increasingly focused both on digital transformation and "security by design," we are also seeing a shift in mindset related to the responsibility for cybersecurity of digital projects and offerings. Increasingly, these responsibilities are being taken on more by the business. There are a number of reasons for this. The organization understands the needs and expectations of its customers, including the need to deliver the best user experience, to deliver as quickly and frequently as possible, to keep services updated (often on a daily basis), and to remain competitive.

This shift in mindset means that there is greater requirement and advantage for cybersecurity experts to work directly with a business. More organizations are striving to instill in leadership roles a greater knowledge of cybersecurity as a strategic driver in their business operations rather than just a separate department or function.

Today's customers have high expectations about the quality of digital experiences. Customers also, understandably, expect organizations to exercise good practices around how their identity information is collected, stored, managed, and shared. Exploitation of customer data by a cyberattacker can significantly damage an organization's reputation, result in penalties and fines and, in some cases, force an organization to close permanently.

In 2020, a Virgin Media database containing the personal details of 900,000 people was left unsecured and accessible online for 10 months. The breach was apparently not due to a hack or a criminal attack, but because the database had been "incorrectly configured" by a member of

staff who did not follow the correct procedures, according to Virgin Media. The customer data was accessed "on at least one occasion" over this period by an unknown user. The unguarded database was first discovered online by researchers at TurgenSec, who then reported it to the Virgin Media's security team as per the National Cyber Security Centre (NCSC) cybersecurity guidelines. Virgin Media is now facing a penalty of £4.5 billion ($6.2 billion) payable to 900,000 customers for allowing unauthorized access to their personal data.

Another big shift is occurring on the operational technology (OT) side. Many of the technologies supporting heavy industry—including manufacturing, utilities, oil and gas, as well as Internet of Things devices in homes and offices—are increasingly reliant on connectivity and data exchange which means additional attack surfaces. The Colonial Pipeline ransomware attack in the United States that made headlines around the world earlier this year, took down the largest fuel pipeline in the country and led to fuel shortages across the East Coast. The attackers gained access to the networks of Colonial Pipeline through a VPN account which was no longer in use at the time of the attack but had not been decommissioned. The account's password was later discovered inside a batch of leaked passwords on the dark web. The account didn't use multi-factor authentication (MFA), and this oversight allowed the hackers to breach Colonial's network using just a compromised username and password.

In February 2021, Centrais Eletricas Brasileiras (Eletrobras) and Companhia Paranaense de Energia (Copel), two major electric utilities companies in Brazil, announced that they had suffered ransomware attacks that disrupted operations and forced both companies to suspend some of their systems temporarily[2]. OT attacks are becoming increasingly more frequent, with higher impact and greater risk.

Because OT infrastructure is normally managed separately to IT infrastructure, OT teams are also increasingly being asked to take ownership of their cyber risk. These shifts provide opportunities for collaboration across different groups with different expertise, working with a common vision. To be successful, organizations need a consistent, unified strategy to manage cyber risk.

DevOps

The global trend toward DevOps and cloud services is good news for organizations seeking to benefit from digital efficiencies and new market opportunities. These trends are also expanding the cyberattack surface rapidly and exponentially. The immediate result is a proliferation of privileges across human and non-human identities.

Most organizations today rely on software engineering to drive innovation and opportunity. While DevOps teams are delivering powerful advantages for their organizations, there is a noticeable and significant increase in cyberattacks against developers and cloud engineering teams.

DevOps teams are also frequently under pressure to deliver quickly. The relentless pace of transformation, combined with the competing need to maintain secure access to infrastructure, systems, applications, and code, can mean that organizations cut a few corners, increasing risk.

Simply telling developers to abide by policies they see as slowing them down may not be very effective. To address this, Verizon developed a centralized, real-time developer dashboard that shows how vulnerabilities are introduced into applications within Verizon's business. This solution helped to convince developers to accept a DevSecOps approach and to nurture a security culture within the organization.

Another effective solution may be to turn the cybersecurity team into DevOps partners. This means that the cybersecurity team will need to learn to communicate in the language of the DevOps team. The cybersecurity team should ideally learn what tools the DevOps team uses and how they work, so that together they can identify workable strategies that are mutually supporting. For example, leveraging the PAM solution to allow developers to securely retrieve credentials when needed, and allow those credentials to be updated and maintained on the backend without adversely impacting their code, is a win-win and prevents hard-coding of credentials.

Other issues to address can include securing DevOps tools, managing software supply chains, and teaching DevOps teams to think like hackers and to understand that they are prime targets. Together, the DevOps and cyber teams can ensure that good practices, like least privilege, MFA, and encryption, become key parts of the software development lifecycle.

The challenges of cloud

In 2020 for the first time, organizations invested more in cloud infrastructure than in on-premises data centers.[3] As a result of the pandemic, almost all organizations have accelerated their plans to adopt cloud services. Cloud providers are adding new services faster than ever to keep up with demand, and organizations are adopting them at velocity, all of which even further expands the attack surface.

Managing privileges in the cloud can be tricky given the dynamic nature of the workloads—autoscaling, spinning things up and down through automation orchestration, making frequent changes. The speed, the complexity and the lack of end-to-end visibility can create numerous opportunities for attackers to exploit vulnerabilities.

According to a recent report by McAfee, after analyzing billions of events in various cloud deployments, the data stored in cloud storage platforms is more exposed to cyberattacks than the data stored in the server farms of organizations. This can often be the result of configuration errors or accidental and uncontrolled sharing by the customer rather than any fault of the cloud service provider (CSP). During the first four months of 2020, perhaps unsurprisingly, McAfee witnessed a surge in attacks on cloud accounts, an estimated 630% increase overall.[4] Organizations need to really understand how their cloud services work and do their part to protect the relevant information.

Leveraging PAM, a few examples of what can be done to reduce the organization's attack surface in the cloud might include locking down the cloud console, giving users just-in-time access rather than full access rights, and responding quickly to alerts of any suspicious activities on the server.

Another important option when using cloud applications and other services is session isolation and management rather than exposing a credential. This means that access occurs via a click, so that even if your endpoint is compromised, an attacker does not get access to that credential.

Steps to success

The first action every organization needs to perform when starting on the journey to secure and improve PAM is to conduct a full inventory of current privileges in the organization. If there are existing business continuity plans that prioritize systems and other information by business criticality, this should be used to determine which are the highest priority accounts for PAM to manage.

The inventory of current privileges needs to include legacy systems, shadow IT, and the organization's ecosystem. It should not be limited to on-premises, or internal staff. Existing repositories should be scanned to see if there are any hard-coded credentials that should be addressed. This inventory will clarify what is there and allow credentials to be locked down, vaulted, and checked in and out. Once this is completed, invalidating expired or obsolete credentials alone will provide a tremendous advantage and significantly reduce the attack surface.

At the same time, living in our digital age means that what the organization has today may change dramatically tomorrow; the ability to continually adapt is an essential aspect of both cyber and organizational resilience. Moving forward, having a seat at the table to evaluate future organizational needs from a cybersecurity perspective should be a priority.

Conclusion

Digital transformation increases the potential for privileged access abuse, but it also creates opportunities to improve, integrate and automate PAM. Maintaining an acceptable level of cyber risk requires that the organization has clarity about which identities, which systems and which data it will prioritize, based on its value to the organization and the impact to the organization if it is compromised. These are business decisions to make based on the organization's entire risk profile, so cybersecurity teams, IT, developers, and other parties should not determine these factors in isolation. The organization and its partners will need to work together to deliver successful outcomes.

Citations:

The Forrester Wave: Privileged Identity Management, Q3 2016

https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/

https://www.srgresearch.com/articles/2020-the-year-that-cloud-service-revenues-finally-dwarfed-enterprise-spendingon-data-centers

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/

About the author:

Erin Casteel

Erin Casteel is a strategic advisor, governance and management system expert, and business architect who helps organizations transform and thrive at velocity in the digital age. She works with organizations to design, implement, run, and improve organizational governance and management systems. Erin also develops cybersecurity and agile service management to create and preserve value. She is a lead architect and author of ITIL 4® and an editor of and contributor to a number of international (ISO) management system standards, including the ISO/IEC 27000 family of standards for information security management.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360