Securing Remote Vendor Access with Privileged Account Security

Table of Contents

Introduction to privileged remote third-party access

In addition to your internal users, typically employees, many external users require access to your network in the course of normal business operations. In fact, 60% of organizations allow third-party vendors remote access to their internal networks.[1] These third parties, including vendors, contractors, consultants and service providers have authorized access to your network, allowing them to change, alter or impact the operational service of your business. This access is privileged access—and needs to be protected to the same (or higher) standards as internal privileged user access. However, as organizations work to secure their networks, they often overlook remote vendor access as a privileged access point that requires tight security controls. The unintended consequence of this approach is a very weak link in security, one that is all too often exploited by attackers to gain powerful access to your network. This paper will explore the implications of third-party access on network security and recommend best practices to strengthen this weak link in IT security.

60% of organizations allow third-party vendors remote access to their internal networks.

Do you know who your remote vendors are?

The first step in understanding the scope of the problem is to identify all of the external users and entry points to your network that are authorized but not fully controlled and managed by the IT organization. This is often a difficult task for IT and security teams because most leading institutions have 200-300 high-risk, third-party relationships at a time.[2] These accounts could be established by the third parties themselves or be embedded in systems hidden from the purview of IT.

While the list of potential third-party users accessing the network is long, here are some common categories of users:

Third-party hardware and software vendors
To provide remote service and maintenance under contract, support engineers access accounts built-in to hardware and software solutions. An example is remote service accounts for large enterprise storage systems, which are created and managed by the vendor and not the organization where the storage system is installed.

IT services providers
Organizations and their employees that provide outsourced IT services, such as help desk support, require access to network resources to reset passwords and complete other administrative functions.

Supply chain vendors
Organizations that provide services, products and infrastructure to support the production and delivery of goods may require network access to fulfill orders, maintain systems or monitor inventory. An example is a Point of Sale (POS) vendor that implements and maintains a system for a retail company.

Services companies
Vendors that provide business services to a company including legal, public relations and others often require network access to be most effective. An example is a web services company accessing the network to build and launch a new website.

1 Global Advanced Threat Landscape survey, CyberArk, 2014

2 Managing third-party risk in a changing regulatory environment, McKinsey & Company, May 2013

External consultants

External business and IT consultants require access to network resources in order to complete projects. These accounts are created by the IT teams, but the credentials are managed by third parties. An example is a management consultant accessing data and reports for analysis during a long-term strategic project.

Whether the accounts used by remote vendor users are created by the third party or the internal IT organization, it is a real challenge for IT to establish and maintain control over the users and credentials. These uncontrolled privileged accounts introduce a significant security risk to an organization, and when left alone, invite determined attackers to enter the network unnoticed.

Most leading institutions have 200-300 high-risk, third-party relationships at a time.

The risk: unmanaged credentials in the wrong hands

When organizations consider the security of remote, external users accessing the network, they often prioritize securing the connection itself using Virtual Private Networks (VPNs) or Virtual Desktop Infrastructure (VDI). While these security measures are a good idea, the misstep happens when the account credentials for the VPN or VDI are put in the hands of the external user, completely outside of the security policies and management of the organization. With no control over the credentials or governing policies, organizations are defenseless against a user's poor credential management tactics including storing passwords in a file (or on paper), sharing credentials or inadvertently exposing them to unauthorized users.

The security (or lack of security) on the user's endpoint is another source of risk to an organization. In the case of third-party access, the originating endpoint is not under the management of the organization's IT team, which means the health and security of the endpoint is unknown. This leads to unknown risk of exposure to malicious software with few preventative or recourse options for the organization.

And, perhaps presenting the biggest risk to an organization, are the accounts created by the third party and existing on the network, unknown to the organization. After all, how can organizations secure what they don't know exists?

Persistent attackers are aware of the weak links surrounding third-party access to network resources, and they compromise these unmanaged credentials or exploit unsecured endpoints to gain entry to your network. Once access is obtained, the attackers employ lateral movement techniques to reach the target asset and execute a successful breach. Therefore, locking down privileged accounts used by external users is instrumental in protecting your network from unwanted access and data breach.

Lock down credentials and keep a watchful eye on activity

Organizations cognizant of the risk associated with third-party access do have options to protect their networks. With appropriate controls and monitoring, organizations can provide third parties the access they need without sacrificing security standards.

Manage and secure credentials

Identifying all third-party users and associated credentials is the critical first step in mitigating the risk of compromised credentials. This means finding accounts provisioned by your organization, and those created by vendors and embedded in systems—accounts you may not even be aware of. Included in this discovery process should be all accounts and credentials assigned to users as well as application-to-application accounts accessed using passwords embedded in the application or SSH keys locally stored in the server.

An effective way to begin the discovery process is to scan the network using a tool designed to identify privileged accounts. CyberArk Discovery and Audit is a free, standalone tool designed to find privileged user and application accounts and credentials. The tool produces a full report including a list of accounts and associated credentials (passwords and SSH keys) as well as account status with regards to company security policy. With this report, organizations have an initial view of privileged accounts accessed by internal and external users.

Once all accounts and credentials are identified, it's time to shore-up any weak spots and areas of potential compromise. In short, regardless of current practices, the privileged accounts and credentials used by third parties need to be put back in full control of the IT organization. An effective approach is to centrally store the credentials in a secure digital vault and implement access controls for remote users requiring access to privileged accounts. Once the credentials are stored in the vault, users log in to the vault to access the credentials they have permission to use. The users can then securely retrieve the password or SSH key, or request a direct connection to the account. This process results in centralized provisioning and deprovisioning of accounts without having to touch endpoints, a key benefit when working with users from remote vendors who frequently change roles.

Once the credentials are stored and managed using the digital vault, regular, automated rotation of credentials by the system reduces the risks associated with stale credentials. Use of one-time passwords can be achieved with rotation of credentials after every use. This automated rotation of passwords and SSH key pairs is a requirement in many compliance regulations and aligns with best practices for securing privileged accounts. Account access can be further protected with multi-factor authentication to the vault and workflow approval processes can be required before the most sensitive credentials are retrieved. With these security solutions in place, external (and internal) users who require access to a system have convenient, secure access to the credential stored in the vault while credential management and control is back in the hands of IT.

The digital vault solution not only secures and controls access to the credentials, it also introduces individual accountability. Now that users have to log in to the digital vault to access a credential, the blind spots around shared account usage disappear, and individual activity can be tracked and reported, bolstering auditing and forensics processes. This is particularly important if credentials are shared between internal and external users; with individual accountability, it's clear who is responsible for an action – someone in your organization or the vendor.

The CyberArk Privileged Account Security Solution includes several integrated components that deliver a digital vault solution to manage and secure credentials required by external users including:

- **Enterprise Password Vault** - secures, rotates and controls access to privileged passwords
- **SSH Key Manager** - secures and controls access to private SSH keys and rotates SSH key pairs
- **Application Identity Manager** - removes passwords embedded in applications and SSH keys locally stored on machines, and centrally secures, manages and rotates them

Working together in any combination, the components of the solution can secure and manage all credentials used by third-party vendors to access the network.

Isolate and monitor the session

Unmanaged endpoints accessing the network provide an opportunity for attackers to install and use malware including keylogging software or other tools to obtain direct access to sensitive assets. The primary tactic to mitigate this risk and secure remote sessions is to isolate all sessions originating outside the network and from unmanaged devices. This isolation can be achieved by requiring connections go through a jump server, which can provide added security by monitoring and recording privileged sessions.

The jump server can be integrated with an existing VPN for maximum protection. Once the remote user connects over the

©Cyber-Ark Software Ltd. | cyberark.com

VPN, he or she then logs into the jump server via a secure web portal. From the web portal, the user selects the target machine to which they need access. Once the target is selected, a direct connection is created from the jump server over a standard protocol such as RDP or SSH, establishing complete isolation between the user's endpoint and the target system. In this process, the jump server communicates with the digital vault to manage who has access to which systems, and can allow access to specific applications, acting as a single control point between all external users and target machines on the network.

The jump server protects the target asset in three key ways:

Blocks the spread of desktop malware. With the use of a jump server, the session is actually running on the isolated proxy server, not on the user's endpoint. Therefore, if an attacker attempts to gain access to an internal network by installing malware on a vendor's or external user's endpoint, the jump server intercepts the spread of malware, protecting the network from infection.

Mitigates the risk of credential theft. The jump server retrieves the credential from the digital vault and initiates the session, which means the user never types in the password and it's never disclosed to the remote user. Therefore, keylogging software installed on the endpoint is ineffective and the password is not susceptible to poor management practices of the third-party user including sharing, writing down or storing passwords in digital files.

Monitors and records every session. Once the connection is made, the session can be viewed and terminated in real time and recorded for future forensics analysis. Also, because the jump server acts as the single access control point, every single session is monitored and recorded. Attackers who exploit the external access of your third-party users will not be able to bypass this critical security control. This central control point can limit the power of the remote user by supporting two-factor authentication, enforcing session duration limitations and integrating with ticketing systems.

CyberArk Privileged Session Manager, part of the Privileged Account Security Solution, is a zero-footprint, agentless solution that acts as a secure jump server. With preventative measures, such as isolation and account controls, account credentials are never exposed to remote vendors and external users, dramatically reducing the risk of attackers compromising credentials to access the network. Detection features, such as over-the-shoulder monitoring and DVR-style recording together with the detailed and searchable audit of user activity, help organizations detect suspicious behavior that indicates the compromise of remote vendor credentials. Working together with digital vault solutions or alone, the jump server solution is quite effective in protecting against attacks originating from third-party accounts or users.

Identify suspicious activity

Adding threat detection capabilities to security solutions for third-party access is critical in order to detect account compromise before real damage is done. At the core, threat detection is based on identifying irregular behavior of users and assets, indicating that the authorized user is not in control of the account. The good news is that external users have definable activity patterns that can be used as a baseline to identify suspicious activity. In the case that an attacker compromises a remote vendor's credential or exploits an account to access your network, anomalies in the remote user's patterns are sure to appear. Analytics tools that learn the typical patterns of activity and continuously monitor user and account activity can identify and alert on suspicious activity. The alerts can be used by IT and security teams to detect and disrupt in-progress attacks, dramatically reducing any damage to the business.

CyberArk Privileged Threat Analytics integrates seamlessly with components of the Privileged Account Security Solution and existing Security Information and Event Management (SIEM) solutions to collect and analyze data on privileged account use. The data is continuously compared to baseline "normal" behavior and alerts are sent to the CyberArk dashboard or the SIEM solution for immediate action by security teams. With a focus on privileged accounts, including third-party accounts, CyberArk Privileged Threat Analytics provides targeted alerts on the most often-used attack vector, privileged accounts.

Accelerating business securely

Allowing external, third-party users from vendors, partners and contractors to access your network is an inevitable part of doing business today. This access facilitates business productivity, allowing external and internal users to collaborate efficiently on projects, address maintenance issues quickly and provide seamless services to your environment. Without this access, revenue opportunities are missed, projects advance more slowly and the chances of system downtime increase. Providing secure, protected and monitored access to your network for external and internal users allows IT organizations to provide the necessary business access without introducing significant new risk.

Conclusion

Remote, external users accessing your network from third-party organizations introduce a risk that can be mitigated. With the proper credential protection, account controls and detection capabilities in place, organizations can minimize the risk of unauthorized users exploiting accounts used by vendors, contractors, service providers, supply chain vendors and temporary workers to gain unmitigated access to the organization. Implementing these controls enables the business to partner effectively with outside parties while maintaining the same security standards across the entire organization.

All rights reserved. This document contains information and ideas, which are proprietary to CyberArk Software Ltd.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of CyberArk Software Ltd.

Copyright © 2000-2015 by CyberArk Software Ltd. All rights reserved. | cyberark.com