WHITE PAPER | APRIL 2016

Closing Network Backdoors

Top Five Best Practices for Controlling Third-Party Vendor Risks

Dale R. Gardner
CA Security Management

Table of Contents

Executive Summary

Challenge

Major breaches at Target, Home Depot, eBay, U.S. Office of Personnel Management and others were made possible by stolen or compromised user credentials, belonging to a privileged user with wide-ranging access to sensitive systems. In nearly two-thirds of cases, the initial breach was facilitated by loose security practices of a third-party—a vendor or a business partner who had access to an internal network. With stolen partner credentials, attackers explored breached IT infrastructure, seeking out privileged accounts that were then exploited to gain unauthorized access to critical systems and cause severe damage to the businesses.

Opportunity

Similar to companies that were breached, many organizations face a frustrating and complex mix of third-party vendors, contractors and business partners with network access to their IT infrastructure and a variety of privileged accounts used to run mission-critical applications. In today's interconnected work, access cannot be completely blocked and privileged accounts cannot be eliminated, so the only option is to better protect privileged accounts from unauthorized users, thus better protecting sensitive information assets.

Benefits

Outsourcing cost savings, quality improvements and efficiencies are made possible by the interconnected enterprise. Restricting network access at the firewall for everyone is no longer an option. Relevant resources must be available to business partners, to reap business benefits. Information security best practices need to be in place to block breaches, while allowing legitimate business activities.

Section 1

Risks Created by Third-Party Access

Today, most organizations have a number of non-employees with some level of privileged access to internal networks and systems. Frequently, the company's information security team may know little to nothing about these people, other than that they work for company's vendors, outsourced service providers or business partners. Typically, these third-party users represent the biggest risk for the enterprise because their accounts are frequently the easiest route to compromise the enterprise. Examples of these beaches can be seen in major news stories about Target, Home Depot and others. A relatively small third-party's compromised user access can be leveraged to gain wider access to the organization's networks and systems — and gigantic damage results. These breaches are not aberrations. According to Troy Leach at the PCI Council, about 65% of breaches can be traced back to a third party.

Regulators are aware of these risks and are working with industry to develop appropriate controls and regulations to address the challenge. For instance, PCI Version 3 of the Data Security Standard introduced new controls aimed at addressing 3rd-party risk. Benjamin Lawsky, New York state's superintendent of financial services, noted **"A bank's cybersecurity is often only as good as the cybersecurity of its vendors. Unfortunately, those third-party firms can provide a backdoor entrance to hackers who are seeking to steal sensitive bank customer data."** As a result, financial services, healthcare and other industry regulators are developing new compliance requirements to reduce risk and improve security.

> "A bank's cybersecurity is often only as good as the cybersecurity of its vendors. Unfortunately, those third-party firms can provide a backdoor entrance to hackers who are seeking to steal sensitive customer data"
>
> – Benjamin Lawsky, Superintendent of Financial Services, State of New York

---

Section 2

Top Five Best Practices for Controlling Third-Party Vendor Risks

Moving forward, controlling and managing third-party access to networks and systems is becoming an increasingly important requirement for both information security risk management and regulatory compliance.

> "Hackers had accessed OPM's networks via credentials stolen from contractor KeyPoint Government Solutions."
>
> Exclusive: The OPM breach details you haven't seen, August 21, 2015

Best Practice 1: Implement Supporting Processes and Controls

Similar to most information security issues, a good starting point is defining processes and controls that help manage risk. This is particularly important for managing third-party risk, because most activity occurs outside the direct purview and control of the information security team. Because business relationships can be established and access may be provided without the knowledge or review of the information security team, the information security team needs to be involved during contract negotiations, so that appropriate policies are developed and enforced, as a part of the overall identity and access management framework.

The simple part of the process is provisioning, de-provisioning and defining appropriate policies for non-employee privileged users. Similarly to other privileged users the following areas need to be clarified:

- User definition and training
- Systems and resources to which access is needed
- Level of privileges needed to perform duties
- Any restrictions to be enforced
- Monitoring, session recording, alerting and session review frequency

Most organizations already have these policies in place for privileged users. If these policies do not exist, they need to be created. The same processes and controls that apply to employee privileged users need to apply to non-employees. Depending on organizational structure and size, IT operations, individuals responsible for identity management or a contracting group typically manage these processes. These groups need to be aware and agree on processes for training, provisioning, monitoring and de-provisioning third-party privileged users.

Security Standards

Generally speaking, security is only as strong as the weakest link. Through a partner's privileged user, the partner's infrastructure and processes become a part of organization's own IT infrastructure. Just one partner with weak controls or poor security can be a conduit for hackers to break organization's protection, as evidenced by the Office of Personnel Management breach that occurred via credentials stolen from contractor KeyPoint Government Solutions. So, from a risk management standpoint, assessment of each partner's security relative to established organizational standards is important. In an increasing number of cases, PCI, HIPAA and other compliance mandates require performance of third-party vendor assessments and outline specific requirements.

Most organizations already have established information security standards. These standards need to apply to third-party vendors. To develop new information security standard, several sources are available:

- Shared Assessments publishes a Standard Information Gathering (SIG) document, to help standardize information security gathering and assessment process
- Office of the Comptroller of the Currency (OCC) publishes broad risk management guidance, with IT-specific sections that can be leveraged
- Federal Financial Institutions Examination Council (FFIEC) publishes documents with relevant standards
- Department of Health and Human Services Security Risk Assessment Tool
- NIST's 800-53 Security and Privacy Controls for Federal Information Systems

- State regulatory authorities
- COBIT or ISO 27002 policy and control frameworks.

Additionally, industry-specific compliance mandates may include requirements for working with third-parties:

- PCI Data Security Standard
- HIPAA HITECH

Implementation, Training and Enforcement

Once assessments and processes are in place, they need to be implemented and enforced by IT, Finance, Legal and the business units who own the vendor relationships, as a normal part of third-party contract definition and implementation. Below are the basic elements that need to be included in third-party contracts:

- Warranties: references to the actual policies and procedures that a vendor commits to enforce, including background checks and training of vendor's employees with access to organization's systems.
- Remedies: Penalties for non-compliance and remediation processes.
- Audit Provisions: Checks and balances available to validate compliance and frequency of audit.

These fundamental risk management provisions need to be incorporated into the relevant parts of the contracting and implementation process. The detailed nature of policy and enforcement vary by business area, balancing risks and costs.

Best Practice 2: Authenticate Users Better

The biggest risk mitigation opportunity where the least amount of cost and effort can deliver the highest risk reduction is in user identification and authentication. As mentioned earlier, roughly two-thirds of breaches can be traced back to inadequate third-party user identification and authentication, including credential management (or lack of it). Generally, third-party organizations tend to be smaller firms, lacking the security maturity and experience of larger organizations. This frequently leads to problems. User credentials can be compromised one of two ways: inadequate strength and management of credentials or inadvertent disclosure of credentials to the wrong person.

- **Weak Credentials:** Even if a strong password is chosen, enforcing password rules and aging can be a tedious process. People, especially smaller vendors, do not practice them. For example, one third-party vendor used the same userid and password credentials for all customers. Once attackers compromised that one set of credentials for one customer, they could simply go through the vendor's customer list (which was thoughtfully posted to the vendor's website) and pick off the rest of the organizations, one by one.
- **Erroneous Disclosure:** According to the recent statistics, the success rate for repeated phishing attempts is close to 100%, after only five to seven attempts. This is a reflection of how sophisticated these efforts have become and the human nature of even the most skilled and sophisticated users. Only one mistake leads to a compromise, as was illustrated in Ukrainian power grid breach in December of 2015. This means that even more skilled business partners may still be prone to phishing attacks.

The best way to protect credentials used to access systems is to proactively manage and control them, by defining and enforcing policies, including

- Complexity
- Frequency of change
- Multi-factor authentication

A best practice for credential management is multi-factor authentication for all third-parties (and internal privileged users). Once an organization is targeted, it is just a matter of time before the credentials used by a third-party vendor are compromised. For example, in the Ukrainian power grid breach, BlackEnergy malware appears to have been delivered to an unsuspecting privileged user via an infected Microsoft Office attachment and then used as an initial access vector to acquire legitimate credentials. The best way to prevent this from occurring is by adding another factor into the authentication process. Several multi-factor authentication options are available. The specific option that is most effective depends on a combination of economics and regulations or compliance mandates. For example, in the US Federal government, there are specific requirements for use of PIV/CAC cards for privileged and administrative users. In other environments, other options are available, including certificates, hardware-based tokens and even software-based tokens or verification processes that leverage a person's cell phone. The economics of multi-factor authentication are very favorable, making the business case easy to build.

Effective third-party credential management relies on vendor's users to have individual credentials, which is not consistent with current business practices in many organizations. In many cases, instead of creating an account for a user, an account is created for a vendor, with an understanding that any of the vendor's employees can use the same account and credentials. This may be easier administratively, but the following problems occur when several people share an account:

- Multi-factor authentication is more complicated.
- Ability to control access to and use of credentials is harder, especially in cases where someone leaves the organization or changes roles. It's just too easy for shared credentials to be leaked or stolen.
- Attribution, the ability to determine which individual took a specific action on the network is lost. If an account is shared among multiple people, there is no way of knowing which one of these individuals performed the problematic action.

Implementing a process where credentials are issued to individuals, rather than vendor, largely eliminates these problems and simplifies the process of on-boarding and off-boarding users. When someone joins the business partner's organization, an account is created and access is provided. That account and access can be terminated just as quickly and easily, when that individual leaves or changes roles. Successful access management and user authentication are not just technology issues, but also people, process and training issues that need addressing when vendor agreements are negotiated and processes are established. Vendors need to provide notification of staffing changes — which is extra work for them — and procedures need to be in place to facilitate vendor reporting of these events. On the whole, the additional administrative effort is well worth the enhanced security and control these approaches deliver. In fact, regulatory mandates require individual-level authentication and access control, because they are so effective.

The last area, which may be atypical in organizations, is a requirement for background checks and identity proofing for third-party individuals accessing organization's systems. Again, this is a risk management issue — the cost involved (both financial and administrative) is generally justified, especially in sensitive environments.

One technology that centralizes and automates password complexity rules, password changes and integration of multi-factor authentication systems is a credential vault. Next lowest-hanging fruit after credential management is the separation of authentication from access control.

Best Practice 3: Separate Authentication from Access Control

On most networks, once a person gains access to the network, he or she has visibility — and potentially access — to a broad range of devices and systems. Among the results of this network architecture are breaches like Target, Home Depot, Ukrainian power grid and many others. They are accomplished using a breach kill chain. With the breach kill chain, the attackers complete a series of steps — sometimes iteratively — to successfully carry out a breach. The attack begins with gaining initial access to a network, often through compromised third-party's or vendor's credentials. Once inside, the attacker can search inside the breached network to find vulnerabilities or additional credentials that can be exploited to gain more and more access, at higher and higher levels of privilege, until they finally reach their ultimate target, as was the case in the Ukrainian power grid breach.

> "All three companies indicated that the actors wiped some systems by executing the KillDisk malware at the conclusion of the cyber-attack. The KillDisk malware erases selected files on target systems and corrupts the master boot record, rendering systems inoperable. It was further reported that in at least one instance, Windows-based human-machine interfaces (HMIs) embedded in remote terminal units were also overwritten with KillDisk. The actors also rendered Serial-to-Ethernet devices at substations inoperable by corrupting their firmware. In addition, the actors reportedly scheduled disconnects for server Uninterruptable Power Supplies (UPS) via the UPS remote management interface. The team assesses that these actions were done in an attempt to interfere with expected restoration efforts."
>
> Cyber-Attack Against Ukrainian Critical Infrastructure
> Original release date: February 25, 2016

As mentioned in Best Practice 2, one way to break that kill chain is by controlling access to the network and making it harder for an attacker to get in, by using multi-factor authentication. Another layer of defense is to limit their visibility and access to resources on the network. Most vendors only need to access to very specific systems. They do not need to access to or even visibility of the whole network or even a sub-network.

Network visibility and access can be limited using physical network segmentation. This is frequently done to comply with a regulatory mandate. By segmenting the network and controlling access, the scope of available resources can be limited. While this can be an effective approach, it has shortcomings:

- Administrative overhead required to set up and maintaining that network architecture
- Vulnerability around connections between different parts of the network - an attacker may find a way to traverse network connections to gain access to their target

A better alternative is using logical segmentation with a privileged identity management solution, such as CA Privileged Access Manager, which can limit access to resources. This solution works by implementing a "choke point" a third-party user has to pass, to gain access to protected resources. This approach delivers a number of benefits:

- **Zero Trust Access Control:** A successful login does not provide access to the entire network. Instead, policies that specify what resources are available to a user are enforced by the system, limiting an individual to just those systems. This approach allows for very tight control to visibility and access — an individual never even sees the resources he or she is not allowed to access. The user only sees a pre-defined list of systems he or she is permitted to see and access.
- **Leapfrog Prevention:** To control lateral movement within a network, the system intercepts a variety of networking commands, such as TELNET or SSH and prevents them from being executed. This capability limits the third-party access only to pre-specified systems, eliminating ways to gain visibility to the rest of the network and attempt to get to other systems.

It is important to standardize and consolidate access methods with a choke point, using either a privileged access management solution or a VPN or some other solution that channels access through known pathways. By defining acceptable paths for external access to resources, monitoring becomes easier. By containing unapproved protocols and directing approved sessions to a pre-defined route, anomalies are easier to identify for further investigation, where SIEM and logging tools can help flag abnormal events.

Best Practice 4: Prevent Unauthorized Commands and Mistakes

Access rights and permissions can be used to limit access to information technology resources. Sometimes, this approach does not offer the degree of precision necessary to really control what someone does on a system. For example, a third-party system administrator may need to login to a server using something like root or admin — some type of highly privileged super-user account. Technical or administrative reasons may warrant this access approach, making for a risky situation. With that level of power, the individual can do just about anything on the system, including wiping it out completely — which is an unacceptable risk for most organizations, even if this person is an employee within the company.

A different approach, using a Privileged Access Management solution provides a more palatable approach by enabling fine-grained permissions control for better managing this type of user. The Privileged Access Management system allows an individual to have sessions brokered on his or her behalf to various target systems using a number of different accounts (e.g. root), each with different permission levels.

Command filtering, blacklists and whitelists can also be used to limit what commands a specific user can perform. A blacklist contains commands that are not permitted, while a whitelist contains commands that can be issued —black and white lists used together, provide a high degree of both control and flexibility. So, that the privileged use can maintain the computing resource, without causing unacceptable damage. An unexpected benefit of command filtering is prevention of inadvertent mistakes. In the example above, the super user may be able to move files, but would not be able to reformat the disk.

Command filters combined with logging facilitates monitoring and alerts, so that the system responds in an appropriate way, when someone attempts to beach one of the filters — it might issue a warning or terminate an offending session. For example, an individual may decide to do some experimentation before hitting limits enforced by command filters — when limits are triggered, the system can generate an alert that prompts an investigation into the individual's actions. Here are some of the possible responses:

- Block and warn the user
- Terminate session
- Disable user account
- Generate alert / alarm to SOC

Best Practice 5: Monitor and Investigate

Some level of monitoring is always required. The specific level and scope of monitoring depend on risk and compliance management considerations.

Even in cases with little intrinsic risk, logging helps troubleshoot and investigate suspicious activity. The basic logging is a basic record of what happened and is helpful in reviewing inappropriate or unauthorized activity. It includes

- Logon and logoff times
- Systems accessed
- Commands issued
- Responses received

In any kind of sensitive situations, monitoring leverages logs to enforce established policies for system access, as efforts to violate these policies merit attention. Various actions can be taken in response to an attempted policy violation — at a basic level attempts to violate policies warrant an investigation to find out what happened. Additional training may be required to help people understand what tasks are expected of them and how these tasks should be performed. A violation may be a simple mistake or it could be an indication of attempted malicious behavior. Monitoring helps capture suspicious events, so that they are investigated.

Investigations are very important, as illustrated by JPMorgan Chase whose staff discovered that it has been breached after investigating one of its vendors.

> "JPMorgan discovered the hackers inside its systems in August, after first finding that the same group of hackers had breached a website for a charitable race that the bank sponsors... It was only after JPMorgan found that the Corporate Challenge website had been breached that it learned its own network had been attacked by the same hackers."
>
> "Neglected Server Provided Entry for JPMorgan Hackers"
> The New York Times, December 22, 2014

For even more sensitive situations, session recording or capture may be needed to provide complete information about what happened in a given session, to assist potential future investigations. A common use case is to capture the full-screen recordings of sensitive sessions. These recording can be later examined, in cases of known policy violations or problems that subsequently arose with a system, to evaluate what happened in the original session. Depending on the sensitivity of the environment, spot checks may be desired. One of the challenges typically associated with session recording is that recording files (and system overhead) can be significant. The other challenge is an action plan for reviewing the recorded sessions. Since both technology and time-based costs increase for session recording, cost-benefit analysis helps to identify situations that are appropriate for this level of investment. As a starting point, it is helpful to identify the following:

- When to record and for how long
- When and how often to review recordings
- What is the recordings retention policy

If you do chose to deploy session recording techniques, several capabilities are important:

- Easy access to metadata about the session — when it started and ended
- The ability to quickly traverse sessions and go to a specific point in a recording
- The ability to highlight "interesting" activity, such as policy violations and sensitive activities.

Highest risk situations may warrant "over the shoulder" monitoring or two-party access, which require another individual watching what a privileged user does in real time. Typically, these extreme-risk situations do not occur with third-parties or other external users. "Over the shoulder" monitoring poses technical challenges. However, in addition, the monitor has to be highly-skilled, so that he or she understands both actions taken and their ramifications on the larger environment. From a risk management perspective, "over the shoulder" monitoring may be appropriate for a very small number of situations.

Typical monitoring includes a two-step process:

- **Real-time response to policy violations:** Several actions can occur — warning the user, generating an alert to a security operations center or shutting down a session or an account.
- **After-the-fact research and analysis:** A review of logs or session recordings to support troubleshooting or forensic investigations.

After-the-fact research and analysis can include efforts to correlate logs and alerts generated by a privileged access management system with other network and security tools for unexpected events. For example, in organizations where a privileged access management solution has been implemented, all administrative activity is centralized in the privileged access management system. If SSH or TELNET session requests come from other parts of the network, they are seen as immediate alerts that something is wrong and are investigated. By eliminating or banning unauthorized administrative tools, suspicious activity is relatively easy to identify. A next-generation firewall can assist with flagging applications or protocols that are prohibited. Other suspicious activities may include access at unexpected times or unusual behavior, like file downloads.

Over time, ongoing manual audits and reviews help to find-tune tools and policy to ignore false positives and automate triggers and alerts to be more effective.

Section 3:

Benefits of Managing Third-Party Risk

No modern organization can be isolated and disconnected from the Internet. Business relationships require electronic collaboration where sensitive information is exchanged between partners. Today, companies use third-party providers for accounting services, credit card processing, legal counsel, retirement plans administration, marketing services, manufacturing and hundreds of other jobs. Electronic collaboration between business partners saves time and money, enables automated processes and systems that improve accuracy, quality and efficiency. Restricting third-party network access at the firewall is not an option. Relevant resources must be available to business partners, to reap business benefits. At the same time, companies face real risks by connecting with third parties.

Security breaches are expensive. According to Fortune magazine, after the late 2013 theft of 40 million payment cards and 70 million other records, Target estimated costs of $162 million, after insurance reimbursements. Sony estimated spending $35 million in “restoring financial and IT systems” following a 2014 breach. Home Depot recorded $28 million in pretax net expenses. The above costs do not include reputational damage and rising insurance premiums. In addition to these “hard” costs, people’s lives are turned upside down. Many people lost their jobs and the remaining people had to work around the clock, investigating and mitigating breaches.

> “Regardless of the way we measure it or whether we look forward or backward, we agree on the central point that companies need to invest in information security.”
>
> Benjamin Dean, a fellow at Columbia University’s School of International and Public AffairsmFortune Magazine, March 27, 2015

Clearly, no company wants to be on the front page of the Wall Street Journal as an example of yet another large breach. The top 5 information security best practices can block breaches, while allowing legitimate business activities, keeping your organization’s information assets and reputation safe.

Section 4:

Conclusions

According to Verizon's 2015 Data Breach Investigations Report (DBIR), $400 million in estimated financial loss resulted from 700 million compromised records. Seventy organizations that contributed to this report documented 79,790 security incidents of which 2,122 were confirmed breaches in 61 countries, with two-thirds of incidents occurring in the U.S. Although the vast majority of threats are still from external sources, internal and partner threats increased slightly between 2013 and 2014. The risks are real, as evidenced by the mega-breach at the U.S. Office of Personnel Management.

The method of [OPM] attack followed a formula: Target a subcontractor in a social engineering attack and steal credentials to gain access to the network. Plant malware on a system and create a backdoor. Exfiltrate data for months, undetected.

The OPM breach also emphasized organizations' vulnerability to social engineering. Government employees and contractors are now subject to security awareness training programs to learn about the dangers of spear phishing and other social media threats.

> "The most innovative and damaging hacks of 2015,"
> CSO Magazine, December 28, 2015

Many risks can be mitigated by using five best practices described in this document that work together to create a layered, stronger, more flexible and more powerful information security defense. These practices include:

- Implement supporting processes and controls defining and enforcing policy for third-party privileged users.
- Authenticate users better by using multi-factor authentication technology so that privileged credentials are harder to compromise, even with social engineering and phishing attacks.
- Separate authentication from access control, so that privileged users have limited visibility on internal networks, limiting possible damage that one user or one set of stolen credentials can inflict.
- Prevent unauthorized commands and mistakes, so that real-time triggers are there as the first line of defense, protecting the infrastructure from malicious attempts and inadvertent mistakes.
- Monitor and investigate suspicious activities to quickly catch breaches, improve training when needed and continuously refine automation and processes to eliminate false positives.

Privileged access management systems have automated features and capabilities that help define, automate and enforce the five best practices described in this paper, across the entire enterprise for physical, virtual and cloud environments, helping organizations implement a consistent processes across systems, applications and devices.

Section 5

References

https://www.brighttalk.com/webcast/9017/156931

http://www.xceedium.com/solutions/privileged-identity-management/432-2

http://www.bankinfosecurity.com/occ-more-third-party-risk-guidance-a-7233/op-1

http://www.bankinfosecurity.com/banks-vendor-monitoring-comes-up-short-a-8103

NYS Financial Services Department April 9 report, "Update on Cyber Security in the Banking Sector: Third Party Service Providers"
http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html?emc=edit_tu_20160301&nl=bits&nlid=59970007

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

http://www.cnbc.com/2015/07/22/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html

How Much do Data Breaches Cost Big Companies? Shockingly Little
http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/ March 27, 2015

http://fortune.com/tag/data-breach/ March 2, 2016

http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/10?itc=refresh July 27, 2015

https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx August 21, 2015

http://www.csoonline.com/article/3018343/security/the-most-innovative-and-damaging-hacks-of-2015.html

Section 6:

About the Author

Dale R. Gardner has worked in enterprise software for over two decades, focusing on areas including network and systems management and multiple segments of security, including identity management, application security, vulnerability management, compliance and network security. A former research analyst and writer, he has defined, built and marketed multiple management and security solutions that enhance operations and help ensure the integrity and reliability of enterprise information technology infrastructure. He currently is responsible for the worldwide marketing of CA Technologies privileged access management product portfolio.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.