FORCEPOINT
POWERED BY Raytheon

Whitepaper

Privileged Users

SUPERMAN OR SUPERTHREAT?
A PRIVILEGED USER RISK WHITE PAPER

This white paper explains why privileged users present a greater risk than other employees, and whether or not your organization could be at risk It also provides best practices and strategies for mitigating the threat of privileged user abuse.

Contents

THE THREAT: PRIVILEGED USER ABUSE

An employee with privileged user access, at a U.S.-based global energy company, was enticed by a foreign company to steal source code and other intellectual property from his employer. As a result of his theft, the energy company lost three quarters of its revenue, half its workforce, and more than $1 billion in market value. In a Skype conversation an executive praised the privileged user saying, "Best man. Like Superman…ha-ha." Their "Superman" turned out to be the energy company's greatest threat.[1]

Figure 1. Privileged User Abuse.

This incident caused such extensive damage one might consider it to be an anomaly, but it is not; it is an all-too-common example of one of the costliest risks companies face daily, that of privileged user abuse. According to a national fraud survey, $348 billion a year in corporate losses can be tied directly to privileged user fraud.[2]

Chief Information Officers across the country are keenly aware of the threat not only to their intellectual property, but ultimately to their bottom line. The risk of intellectual property theft isn't limited to a certain industry. It happens across the board from the financial sector to energy and healthcare to the federal government. In fact, the federal government is so acutely aware of this risk, they recently issued a memo renewing their efforts to thwart privileged user abuse.[3] The concern in the commercial market is no less than that of the government, and a U.S. survey of IT practitioners showed 45% of respondents believe the threat will continue to grow (and another 43% believe it will remain the same over the next 12-24 months)[4].

Aggressive federal regulations on commercial companies are compounding the cost of governance, risk, and compliance [GRC]. The impact on market values, reputations, and civil liability may never be fully comprehended.

This paper will help identify who privileged users are in your organization. It will also explain why privileged users present a greater risk than other employees, and whether or not your organization could be at risk. Finally, it will provide you with best practices and strategies for mitigating the threat.

WHO ARE PRIVILEGED USERS?

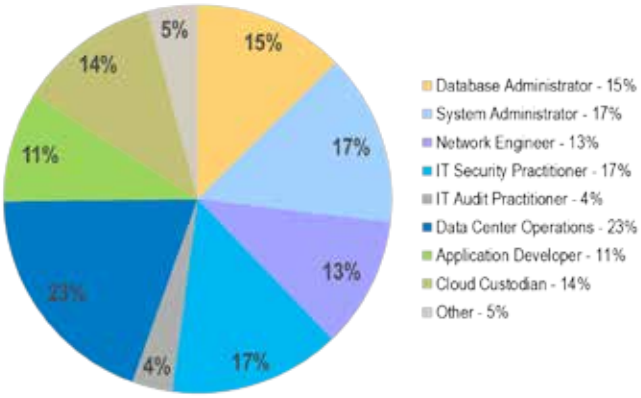

Figure 2. Examples of Jobs that have Privileged User Status[5]

Privileged users are typically associated with a company's IT department and can include database administrators, network engineers, IT security practitioners, etc. (see figure 1). However, across an organization there may be other privileged users that should not be overlooked. A privileged user can be anyone that has elevated access to data, systems and computer assets within a company, from account managers to corporate executives. Damage caused by privileged users is the most extensive, the hardest to mitigate and the hardest to detect as it is done by authorized users doing things they are authorized to do. They are often very technically savvy and have elevated access to systems, making it easy for them to cover their tracks. In the energy company's case, the breach was detected but many businesses aren't so lucky; cases of fraud and theft by privileged users often go undetected and unsolved.

1 NBC News August 06, 2013, Carl Sears, Michael Isikoff URL: http://investigations.nbcnews.com/_news/2013/08/06/19566531-chinese-firm-paid-insider-to-kill-my-company-american-ceo-says

2 ACFE Report to the Nations on Occupational Fraud & Abuse, Association of Certified Fraud Examiners Inc., 2012

3 Information Protection and Insider Threat Mitigation Procedures, Office of the Secretary of Defense, July 12, 2013

4 Privileged User Abuse & The Insider Threat A survey of 693 IT operations and security managers, Ponemon Institute, June 2014

5 Ponemon Institute, June 2014

WHY IS THE RISK SO GREAT?

Because privileged users have greater access and are limited by fewer controls they have access to more of their companies' intellectual property, such as corporate data or confidential customer information (like the foreign company's "Superman"). They may also have access to company computer assets that an average employee does not, for example: laptops, USB devices, Removable HD, etc. Having access to these assets may enable bad behavior in the privileged user, aiding in the mentality that they are somehow "above the law," and not subject to the security restrictions that apply to other employees. Other factors that contribute to a privileged user's potential to cause intense damage are:

- They generally operate at a higher level on the network which provides them with access to enterprise information.
- They know how to operate around and routinely defeat standards and technical controls.
- They are authorized to make changes and access data at very high levels.
- There is often inadequate or no monitoring of privileged users.

A Ponemon study[6] of 693 U.S. IT operations and security managers found that 73% of respondents think it is very likely or likely that privileged users believe they are empowered to access all the information they can view. A similar percentage (65%) said they believe that privileged users access sensitive or confidential data because of their curiosity.

The same study also found that the following practices occur in many of the global organizations represented in the study:

- Not revoking privileged access status after the employee's role changed, and providing everyone at a certain level in the organization with such access.
- IT operations is primarily responsible for assigning, managing and controlling privileged user access rights. However, business units and IT security are the functions most often responsible for conducting privileged user role certification.
- Privileged access rights that go beyond the individual's role or responsibilities are often assigned.
- There is an inability to create a unified view of privileged user access across the enterprise.

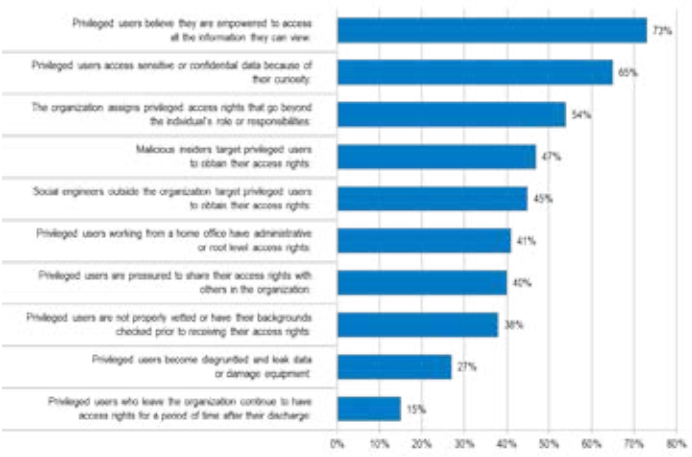

Figure 3. Indicators of privileged user access governance issues Very likely and likely response.

PRIVILEGED USER ABUSE IS UBIQUITOUS

Privileged user abuse isn't just a problem within the government, banking and finance sectors, and it's not just a problem for IT and telecommunications.

The reality is that privileged user abuse can be found in almost any organization. Figure 4 shows the percentage of insider abuse by industry[7]

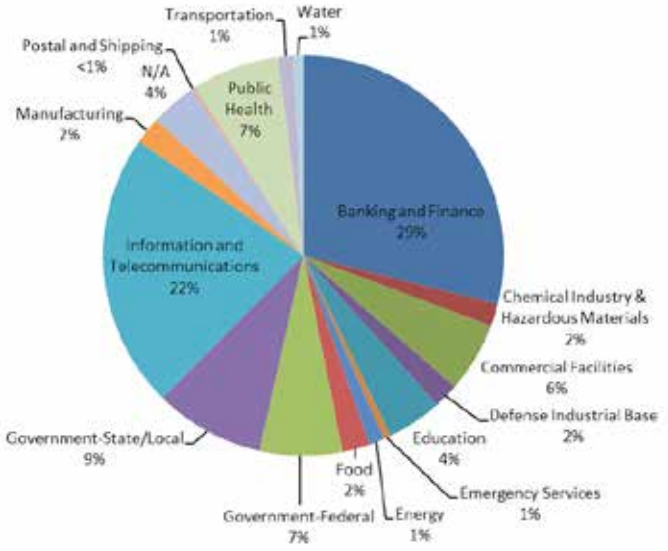

Figure 4. Percentage of insider abuse by industry.

6 Ponemon Institute, June 2014

7 D. Cappelli, A. Moore, R. Trzeciak, The CERT Guide to Insider Threats: How to Detect, Prevent, and Respond to Information Technology Crimes. Addison-Wesley Professional. 2012

MITIGATING THE RISK: THE MYTHS, THE REALITY

The best approach to mitigating privileged user abuse is a comprehensive and layered approach that implements best practices, involves process and technology and, most importantly, involves a better grasp on the people as well as the technology. It is a common myth among IT management staff that auditing privileged user activity is too difficult and complicated. The truth is that privileged user auditing does not have to be a complicated technical challenge if the auditing and monitoring solution is flexible, policy-based, and provides irrefutable attribution to a particular privileged user. The knowledge alone that your organization uses such auditing and monitoring technology is a huge deterrent against privileged user abuse. Many studies have been done to help identify best practices for mitigating the risk of privileged user threats. The following include guidance from the CERT Insider Threat Program:

1. Identify and review privileged user accounts on your network. Adopt a new mindset that reduces the number and types of privileged accounts within the company.
2. Develop a strategy that protects against internal privileged users, and not just external threats.
3. Train employees in the proper use of elevated access privileges, including logging out after performing tasks that require them.
4. Determine who receives privileged user accounts through well-defined policies controlled by business or application owners.
5. Limit the use of shared privileged user accounts.
6. Use an automated or privileged account management (PAM) tool to administer and monitor privileged user accounts.
7. Monitor PAM tools to ensure they are working properly.
8. Put time limits on privileged accounts.
9. Limit the scope of privileged accounts: only give access to systems and data necessary to complete specific job functions.
10. Enforce separation of duties and least privilege. Separation of duties implies that no one employee can perform all privileged actions for a system or application. Least privilege implies that employees are granted only the bare minimum privileges needed to perform their jobs.
11. Implement strict password and account-management policies and practices. This should be enforced for all users, including administrators and other privileged users.
12. Log, monitor, and audit employee online actions. Organizations need to be vigilant about what actions privileged users are taking, and should use a variety of logging and monitoring techniques.
13. Use extra caution with system administrators and privileged users. Because these users are often granted the "keys to the kingdom" in terms of access and capabilities, additional safeguards often need to be implemented to adequately monitor and manage their behavior.[8]

PRIVILEGED USER TECHNOLOGIES

When it comes to mitigating this risk, having a layered defense by using multiple technologies is vital. There are a variety of tools that address different aspects of privileged user security, but there is no single technology that fully mitigates the problem. Gartner identifies solutions used for privileged account management (PAM) as a set of technologies enabling enterprises to address these specific needs:

- Control use of (usually privileged) shared accounts — shared-account password management (SAPM) tools.
- Allow users granular, context-driven and/or time-limited use of superuser privileges
- Superuser Privilege Management (SUPM) tools
- Manage privileged sessions (such as control outbound traffic and system-to-system "hops")
- Monitor use of shared accounts and superuser privileges with fine granularity.[9]

Some technologies being used:

- **Data Loss Protection (DLP):** Watches movement of data across the network. It is important to keep in mind that when you are dealing with privileged user abuse the data may never traverse the network. DLP solutions can't stop privileged users from destroying or corrupting data.
- **Security Information and Event Management Systems (SIEM):** Can alert companies of unauthorized access to data but they can't prevent a breach.

The ability to monitor privileged-account activity is essential, whether or not PAM tools are deployed. DLP and SIEM technologies can monitor data and data movement, but they are fundamentally content and context-blind and unable to monitor user activity. There is apparently no DLP or SIEM solution that has been created specifically for the privileged user threat and trying to press them into service to mitigate the risk often proves inadequate and could be cost prohibitive.

8 George J. Silowash, CERT Insider Threat Attributes and Mitigation Strategies, CERT, July 2013

9 Ant Allan, Perry Carpenter, Gartner, Ten Best Practices for Managing Privileged Accounts, Published: 30 May 2012, Pg 1, "Recommendations" Refreshed: 19 November 2013

Referring to a recent Insider Threat Report10, Jon Oltsik, Senior Principal Analyst at Enterprise Strategy Group, said, "The data is clear – IT decision-makers are concerned about insider threats and data breaches, but tend to rely on perimeter and network security focused tools today, rather than securing the data at its source. What this research highlights is that large organizations need a data-centric security strategy. Insider attacks are increasingly difficult to prevent and detect, and the research findings reveal the need for a change in approach." The same study found only 40% of organizations are monitoring privileged user activity.

FILLING THE GAP: MONITORING PRIVILEGED ACCOUNT ACTIVITY

Key to mitigating privileged user abuse is the ability to determine context and intent, which can only be accomplished by monitoring human behavior. Forcepoint™ SureView® Insider Threat is a flexible, policy-based end user auditing and monitoring tool that provides irrefutable attribution to a particular privileged user. It provides context and intent through DVR-like playback that enables the operator to discern end-user intent. SureView Insider Threat's Privileged User Monitoring and Auditing (PUMA) Policy Pack is based on business policies and best practices for detecting and deterring privileged user abuse. Deploying the PUMA Policy Pack provides enterprise-wide visibility into privileged user activities.

Designed by a team of domain experts who have spent their careers in information protection, SureView Insider Threat's PUMA Policy Pack includes over a dozen policies, identified by companies and the federal government, as vital to mitigating the privileged user threat. For example, in the case of the energy company, the Chief Engineer downloaded the valuable source code to a thumb drive and then emailed it to the foreign firm. Since SureView Insider Threat PUMA policies monitor USB usage, despite the fact that he had privileged user rights and permission to access the source code, his activity would have been captured. As soon as he used the USB an alert would have been sent, and an investigation would have ensued. In addition, with SureView Insider Threat's DVR like capability that provides an over-the-shoulder view of user activity, the engineer's communication with the Chinese company would quickly have been discovered, and would have made it impossible for him to lie about what he was doing. With the PUMA policy pack in place, SureView Insider Threat could help detect and mitigate an incident such as this.

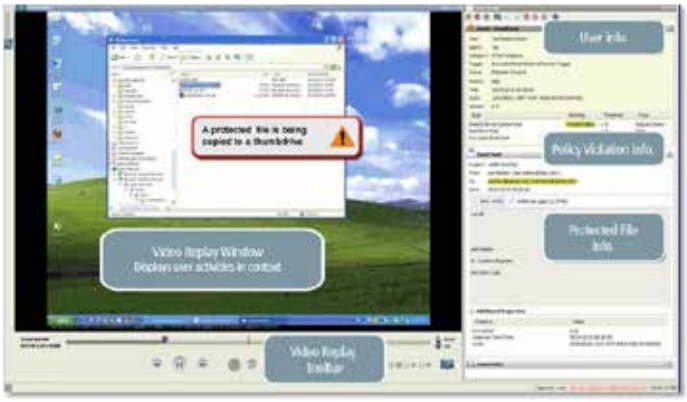

Figure 5. SureView® Insider Threat is a powerful endpoint audit and investigation solution that detects violations across all vectors of communication and provides DVR-like incident replay.

With the SureView® Insider Threat PUMA Policy Pack You Can:
Approach Compliance with Confidence: Superior security that helps you apply the "trust but verify" principle to how you manage and implement oversight for your organization's privileged users:

- **Minimize Privileged User Threats:** Monitor who is accessing your most sensitive assets with out-of-the box policies based on best practices and years of experience with the ability to fine-tune or create new policies to meet your organization's needs
- **Mitigate Risk to Enhance the Bottom Line:** Prevent the loss or destruction of intellectual property and other information assets

The privileged user threat shows no signs of diminishing, in part because of economic pressures that have forced companies to try and do more with smaller staffs. This leads to stressed-out employees who could be more susceptible to cutting corners and cavalier about their use of elevated access privileges to the company network.

SureView Insider Threat's Privileged User Monitoring and Access (PUMA), policy pack provides a new approach to managing the privileged user threat. PUMA relies on monitoring human behavior to determine the context of the behavior and people's intent and uses automated tools to keep an eye on privileged user activities.

10 2013 Vormetric/ESG Insider Threat Report, The Enterprise Strategy Group, Jon Oltsik, Senior Principal Analyst

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #IIS2013-238 [WHITEPAPER_PUMA_SUPERMAN_OR_SUPERTHREAT_ENUS] 200032FED.011416