When admins go bad
- Preparing for the insider threat

Onion ID

Contents

Executive summary

It seems that almost every day we read about another cyber-attack on a world-renowned organization. Indeed, the frequency and sophistication of data breaches of all types is on the rise. From financial and healthcare records to intellectual property and other classified information, data breaches show no sign of subsiding. This constant increase in volume and severity of cyber-attacks can be attributed to several different factors, both external and internal. Today, no organization is immune. Basically any organization that stores sensitive information about their customers and employees, intellectual property or any other information considered valuable, will be, at some point, a target of a cyber-attack.

Insider threat has always been present in every organization. In the last couple of years, the changing trends in the workplace have resulted in insider threat becoming a number one challenge for C-suite executives. While almost all organizations allocate considerable resources and focus their efforts on protecting their network from the external threats, it is the insider threat that poses the biggest risk to cyber-security.

The change to a more flexible and autonomous workplace allows employees easy access to their organizations´ sensitive information. While most organizations are aware of this change and the increased risk of insider threat, most of them have still not done much in order to mitigate this risk, and by doing so, they have created additional opportunities for cyber-attacks. Insiders can attack in five different ways: IT sabotage, fraud, theft of intellectual property, national security espionage and employee negligence.

In order to successfully prepare for insider threats, organizations need to implement a layered defense approach that will be able to detect and prevent them from occurring. Some key layers of such defense mechanism include: taking an inventory of business´ assets, documenting policies and controls, monitoring suspicious behavior, implementing proper access management and segregation of duties, being extra cautious with system administrators, logging and monitoring employee access, and devising a plan to respond to insider threats.

The purpose of this white paper is to inform business owners of the increased risks in insider threats, the different types of attacks and behaviors that these insiders exhibit, as well as some controls that business owners should use to prepare themselves and mitigate such threats. Business owners are encouraged to review their existing plans so that they are sufficient enough to mitigate the constantly increasing risk levels of insider threats.

Definition of insider threats

While most organizations put considerable resources on protecting their network ecosystem, they are often not aware that the insider poses an even bigger threat to their cyber-security. From ordinary employees to executives and IT administrators, there are many people who have legitimate access to information that if exposed to public, could result in serious ramifications to their organization´s business – or even its survival.

When talking about cyber-security, most people consider it to be a highly technical field where highly-skilled IT professionals are trying to defend their organization from attackers with similar skill levels. While this “definition” of cyber-security is not far from the real thing, it forgets to include the most important aspect of every security out there: the human.

Most people have a tendency to trust people they know which leads them to share their credentials or other information that they should keep strictly for themselves. Trust is an important element for every organization. There are many reasons why employees need to have access to sensitive and confidential information and because of them, there is a need to associate a level of trust with that access. To properly understand and manage that trust is one of the most critical and difficult challenges in dealing with insider threats.
In order to properly prepare for insider threats, we first need to understand the definition, causes and types of insider threats. An insider threat is defined as “a malicious insider who is a current or former employee, contractor, or business partner who has or had authorized access to an organization´s network, system or data, and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization´s information system”.

While insider threats may be from malicious insiders who intentionally want to harm their organization either for their personal gain or as an act of revenge, insider threats can also be caused by trusted employees who unintentionally, through negligence, bring reputational and financial damage to their organization.

According to Jeffrey Jones and Ryan Averbeck from CSO Online, there are three types of insiders:

Trusted unwitting insider is an employee that has an appropriate and authorized access to the organization´s network but lacks judgement or is careless in doing their job. For example, this type of insider can find a memory card and put it into their computer to find out to who it belongs to. If the memory card has been left deliberately by an attacker, it would have installed malicious software on the network which would give an attacker the way to gain access to the organization ´s network. Similar to the trusted unwitting insider, the trusted witting insider also has authorized access to the organization´s network but chooses to intentionally give access to privileged information to third parties for personal gain. The untrusted insider is a person who does not have legitimate access to the organization´s network but takes the credentials and role of a trusted employee.

Insider threats have always been here but in the last couple of years they have become top priority for executives that need to devise a clear and concise plan that will help to reduce and mitigate their effect. Employees, especially network administrators, have almost endless opportunities to access their organization´s private information and steal, modify, or even destroy information that is confidential and valuable to the organization. When trying to understand the cause behind insider threats, there are several trends that have contributed to their growth.

The evolution of technology has changed the classical workplace into one that is highly distributive and mobile. Information is everywhere, making it easy for employees to access all types of information online, from a diverse range of devices and from every place with a valid Internet connection. The lower cost of online data storage has made it cheaper for organizations to store all their data as opposed to sorting through all data and storing only the one that is necessary. Furthermore, because of this decrease in cost, data can be easily hacked by malicious attackers.

"What's made public is only the tip of the iceberg. "

- Dawn Cappelli, technical manager, CERT threat and incident management team

"I've been a systems engineer, systems administrator … When you're in positions of privileged access like a systems administrator for the intelligence community, you're exposed to a lot more information on a broader scale than the average employee"

- Edward Snowden, Former infrastructure analyst at the NSA

Why are insider threats difficult to detect?

As more and more people are becoming highly "literate" in IT, the sophistication of the attacks and their occurrence has greatly increased, and organizations find it hard to prevent them, or even to discover trails of data leaks once the attacks have occurred. Since the amount of data that organizations store has increased, the value of that information has increased, as well. This has given insiders more incentives to abuse that data.

While the evolution of technology and workplace has made organizations highly vulnerable to insider threats, most organizations are still doing nothing on the subject. Organizations have implemented a high level of technology for keeping outsiders out, but this technology does a very poor job in stopping insiders to wreak havoc on their data. While most organizations will agree the high level of risk that insider threats pose, most of them will state that the likelihood of these threats happening to them is very low. On the other hand, most CSOs recognize the importance of protecting their organizations from insider threats but feel that they are too difficult to successfully manage.

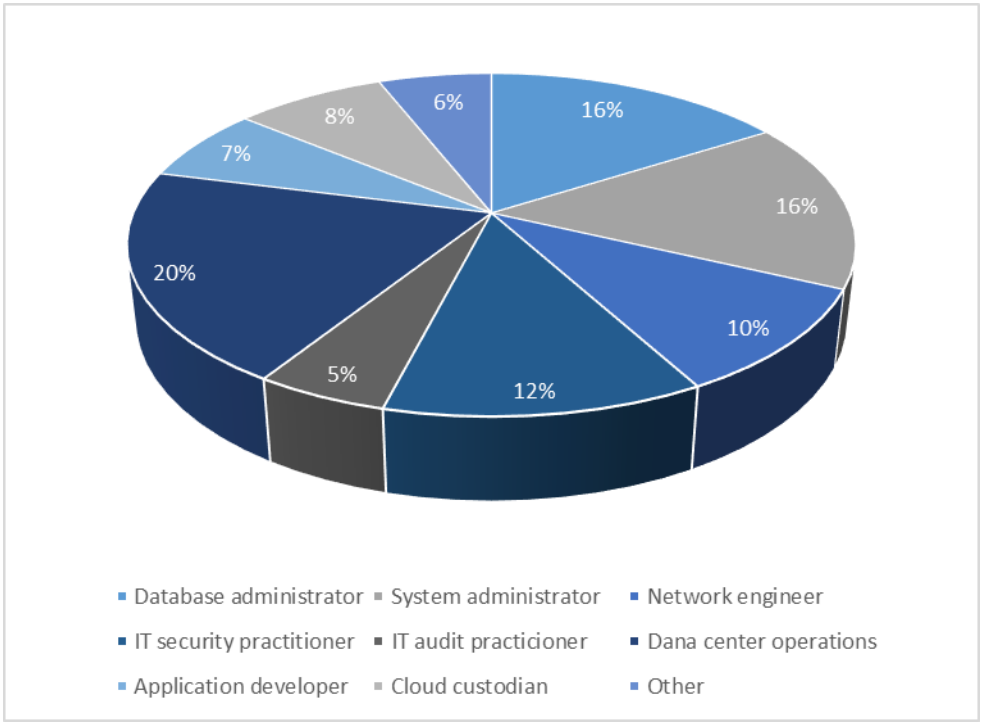
CSOs and other security professionals can feel completely powerless in their efforts to defend their organizations from insider threats simply because insiders can gain access to the network without passing through the perimeter. In case when the insider threat is caused by a trusted witting insider or an untrusted insider, the attack is even more difficult to detect and mitigate. These insiders tend to put a great deal of time and effort in planning their attack and do a good job in covering their tracks. Additionally, their actions can be provoked by many different reasons that are often hard to predict.

Even the FBI has long time ago recognized the concern about threats from administrators and other employees with privileged access to data, both in government and industry. This concern goes so far that it has its own website at the FBI. Additionally, a survey conducted by Ponemon Institute showed that 88 percent respondents recognize the potential danger of insider threats and that the severity of these threats is likely to increase. At the same time, they also said that they find it hard to identify what specific threatening action looks like.

Unlike external threats, the situation with insider threats is more nuanced. With an almost 90 percent of those surveyed in Ponemon Institute report clearly stated that they understand the need for better protection against insider threats, only 40 percent of them had some budget to allocate in protecting their organizations from insider threats.

One of possible reasons behind these staggering results is the fact that organizations find it hard to explain the ROI spent on protection against insiders as the number of data breaches caused by insiders is substantially lower than the number of breaches caused by external threats. However, the damage caused by insider threats is considerably higher.

According to several research studies on the subject of insider threats, it is more expensive to fix damage done by insiders than the damage caused by external cyber-attacks. Therefore, it is critical for organizations to recognize the potential damage from insider threats and shift their focus towards implementing a solution that will proactively prevent and detect these threats.



This chart illustrates the most common positions that require privileged access to sensitive data and networks.
Source: Ponemon Institute

Auditing access regularly

As the results of Ponemon Institute report have shown, most organizations do not have a way to continuously audit access that would help ensure that only authorized employees have access to their systems and confidential information. Even when organizations have some type of auditing tool in place, the sole volume of log data can make it difficult and time-consuming to go through the data and identify breaches and potential threats.

Still, the biggest problem is the fact that most organization look at cybersecurity as a completely “IT thing”. This approach does not only increase their exposure to attack but it widens the gap between those in charge for cybersecurity and those whose job is to ensure a return to investors and shareholders. However, with the high amounts of dollars in damage from successful cyber-attacks, governance is still very important.

U.S. states and foreign governments are responding to the increasingly pressing issue with a wide variety of laws and regulations for data breaches. One of these responses has been made by the U.S. Securities and Exchange Commission (SEC) who recently updated guidance applicable to their registrants. These guidelines are the new frontier in cybersecurity and send a strong signal to organizations to take their cybersecurity efforts very seriously. However, addressing the SEC guidelines is easier said than done as many organizations find it difficult to determine the “what, when, and how” of cyberattacks.

In order to properly address insider threats, it is important to properly define risk factors that all organizations face when trying to reduce the risk of these types of data breaches:

INEFFECTIVE MANAGEMENT OF PRIVILEGED USERS

All organizations have administrators that possess full access to their systems and information stored on these systems. This does not only pose a risk to cyber security, but it can also make compliance more difficult. Sharing administrator passwords is yet another common issue that can lead to unauthorized access, as well as a complete inability to identify who performed which action and on what system.

INAPPROPRIATE ROLE ASSIGNMENT

To properly manage user roles and entitlements is one of the biggest challenges for many organizations. Having roles that overlap or entitlements that are duplicate or inconsistent can easily result in unwanted access and loss of confidential information. Additionally, not having an option to automatically de-provision users can lead to orphan accounts that insiders can use to wreak havoc.

BAD IDENTITY MANAGEMENT

In order to successfully protect from unauthorized access to their systems and data, organization need to have strong control over identities, access and use of information. While most organizations have some controls in these fields, only a small number of them has a unified approach that would address all of them.

There is a tendency to give (tech) people more privileges than they need because you never know when they'll be helping someone else out.

- Larry Ponemon, chairman, Ponemon Institute

With the right security controls, organizations can significantly reduce the risk and potential damage of insider threats.

The key is to have a solution in place that will ensure the right balance between employee enablement and control, while keeping them accountable for their actions.

In order to successfully achieve this, organizations need to have a solution that will allow them to carefully manage identities, access and data, from identity management, to governance, privileged identity management and data protection.

Onion ID

INADEQUATE AUDITING

Most organizations do not have a way to continuously audit access that would ensure that only authorized employees have access and that their use of information is according to organizations´ policies.

COMPLEX AUDIT LOGS

Even when organizations have auditing tools in place, the complexity and sheer size of audit logs can impede with investigation and detection of insider threats and data breaches. The process of logging all IT activity is the first step and thus the most important one in mitigating insider threats.

REACTIVE APPROACH TO INSIDER THREATS

Most organizations will agree that the prevention is better than a cure, and while this is true for their dealing with external threats, they still rely on a reactive approach for insider threats. While a reactive approach can help in investigation of the breach, it will not prevent the attack from happening and causing damage.

Onion ID is a cloud-based SaaS security solution that gives organizations the ability to control access across all their properties.

INFRASTRUCTURE ACCESS MANAGEMENT

Onion ID makes sure that only employees get access to organizations´ Cloud Servers and Containers. With a zero software agent approach no server modifications are needed.

DYNAMIC PRIVILEGE MANAGEMENT

With Onion ID, organizations can easily specify which employee can access what on a website or server. Each action is risk scored using machine learning to detect and prevent threats. Policy setup is easy, flexible and no server or website changes are needed.

ACTIVITY MONITORING

Organizations can easily find out which servers, applications and websites employees are using, as well as have access to detailed reports on alerts and invalid actions. With employee session recording, time to compile forensic and compliance reports is considerably reduced.

LICENSE MANAGEMENT

Organizations can get detailed reports on how well their employees are utilizing money spent on cloud services and identify accounts that are not used. With Onion ID, organizations can reduce their threat risk profile and costs.

INVISIBLE IDENTITY VERIFICATION

Onion ID helps employees get access to what they need without putting roadblocks. Two Factor Authentication can be a nuisance. With Onion ID, there is no need for 8 digit code login and no hardware to carry. With multiple choices like Geofencing, Geoproximity, Touch ID, Onion ID conveniently merges security and usability.

USER MANAGEMENT

With automatic password resets and LDAP/AD integration, Onion ID makes life easier by integrating with organization´s central directory to maintain a single source of truth. Templates help to automatically create user accounts for new employees and disable accounts for the ones that are no longer employed.

Onion ID

Website: https://www.onionid.com

Headquarters: 3526 Investment Blvd.
Suite 213
Hayward, CA 94545
United States

E-mail: sales@onionid.com

Phone: +1(888) 315 4745