Veriato

How UEBA

Reduces the Threat of Insider Data Leakage

The benefits of User and Entity Behavior Analytics in assessing employee behavior

By Derek A. Smith (CISSP)

www.veriato.com

While organizations invest significant resources to stop hackers from getting company data, the greatest risk to organizational data security are the so-called insiders.[i]

WHY INSIDERS ARE THE GREATEST RISK

Consider different potential threat actors[ii] against your home. Everyone knows about the robber – and we invest in locks, security devices, and even acquire insurance because of them. Robbers are, more likely than not, financially motivated. As such, we would expect them to seek out high-value objects that can be easily carried away. The robber is, of course, an outside threat to the home. The likelihood of your home being hit by a robber in any given 12-month period is about 3%. [iiii]

Another potential outside threat actor is the organized crime syndicate. Because of their access to sophisticated means, the syndicate could initiate and conclude an attack on the home and yet never step a foot inside it. Rather, they could attack through your home computer network or even your IoT devices and access your banking, credit, and investment accounts. The attack will be over before you are even aware that you have been cleaned out. Again, the organized crime syndicate would be an outside actor.

THE GREATEST THREAT

"In general, the greatest data security risk is posed to organizations by insiders, as they have access to sensitive information on a regular basis, and may know how that information is protected. If they want to steal it or leak it, they can usually do so with far greater ease than outsiders. Furthermore, insiders may also accidentally leak data or otherwise put it at risk – something that outsiders typically cannot do. Whether by attaching the wrong file to an email being sent, oversharing on social media, losing a laptop or USB drive, or through some other mistake, insiders can put an organization's data at risk with little effort.[i]

- Joseph Steinberg
  Cybersecurity expert

EXAMPLES OF INSIDER DATA LEAKS

February 2016 – A payroll department employee of Snapchat **released the personal protected information of around 700** employees after receiving a phishing email supposedly coming from the CEO Evan Spiegel.[vi]

June 2016 – A city of Calgary employee mistakenly **leaked the personal information** of approximately 3,700 city employees.

June 2012 – After learning that he was to be terminated, an EnerVest network engineer **intentionally reset the energy company's servers** to their factory settings. As a result, EnerVest was unable to conduct normal business operations for 30 days.[vii]

A third potential outside actor against the home is the terrorist hit squad. While the probability of being successfully targeted by terrorists is only about 1 in 20 million , the potential damage they could inflict against the occupants is catastrophic.
Each of these outside threats to your home has a couple of distinct disadvantages: (1) he or she need to find you to attack, and (2) he or she needs to gain access to the occupants and home from the outside – past all the security measures which may be in place.

Consider, however, the home nanny. For the nanny to do her (or his) job, she needs access to the home. Precisely because the nanny has insider access, she will learn where the family keeps their sensitive assets, the value of those assets, and the best times to initiate an attack that may be more costly than all the potential outsider attacks combined. The nanny does not need to find a covert way past the home security in place – she has a key to the front door and the code to the security system.

However, if a threat is caused by the "nanny" – that is, the inside actor – the chances are it will not be realized because of any malicious intent. Research indicates that most insider threats are actually the result of "human error" (in about 87% of cases), a lack of awareness of security issues (82% of cases), or an inadvertent introduction of malware through personal devices (82% of cases).[V] Nonetheless, even though every organization passionately guards against the outside cyber intruder, it is the inside actor – the "nanny" – who is the most worrisome actor when it comes to data leaks.

INSIDE ACTORS MORE LIKELY TO LEAK DATA

Data leaks are defined somewhat more broadly than a data breach. A breach is what happens when data has (potentially) been viewed, stolen, or used by unauthorized persons. A leak, on the other hand, is the unauthorized transfer of data outside the organization's IT system.

Most data leakages are the result of human error or carelessness.[vi] However, leaks may be intentionally caused by rogue employees or other insiders. [vii]

To put the potential for insider data leaks in perspective, consider the following:

There is a 1 in 3 chance that an organization will realize a data breach from an outside attacker.[Viii] However, the average organization experiences 3.8 insider incidents per year.[ix]

The average total cost of an outsider data breach is $4 million. However, the average total cost of the insider attack is $4.3 million.[xi]

Looking at the annualized cost of insider vs. outsider incidents, outsiders cost the average organization $1.33 million per year. By sharp contrast, insiders cost the average organization $16.34 million.

How Organizations are Addressing Insider Data Leaks

Most organizational cyber defenses are geared toward mitigating the outsider attack, monitoring assets, and creating event logs. While the vast majority of attempted attacks are thwarted at the gates, there is still room for improvement.

However, when the threat – malicious or otherwise – exists inside the security perimeter, the strength or effectiveness of the outer defenses are of little importance. For example, the company's firewall may effectively stop the majority of inbound hackers, but it may explicitly be set to allow outbound emails. Thus, while the outside attacker may have difficulty getting at sensitive or confidential data, it does little to prevent the company employee with the proper authentication credentials from accessing confidential and sensitive company data during the ordinary course of the business day and emailing that information to any number of recipients outside the company.

Stopping insider data leakage while still allowing legitimate use of and access to the company's digital assets is a challenge. The most common means which companies are attempting to stem the tide include:

1) **Employee Training.** While the potential rogue employee or corporate spy are significant security concerns, the majority of insider data leaks are caused by human error or carelessness. A robust and continuous employee cyber security training program may help make employees less susceptible to social engineering, phishing, or other means of making the insider an unknowing, complicit partner.

Training may also serve as a deterrent to the would-be rogue insider. If employees know what constitutes IP theft or data leakage – and that the company will prosecute intentional and unintentional digressions from its security policies – they may be less tempted to risk breaking the policies.

2) **Network Monitoring**. Monitoring if an employee is concurrently logged into the IT system from geographically separate locations, or is logging on while on vacation may provide an indication that an insider incident may be in progress.

3) **Outside Contractors**. Of those insider incidences which are malicious, the majority are motivated by financial gain, espionage, or professional revenge. Outside contractors, while posing their own set of security concerns, will not generally be subject to the same motivations as insiders.

4) **Information Segmentation**. Just as companies implement separation of duties to prevent financial fraud, segmenting data and network access on a minimalistic, need-to-have basis may mitigate insider data leakage.

How UEBA & UAM Reduces Insider Data Leakage

User and Entity Behavior Analytics operates on the well-established psychological principle that individuals' behavior and language patterns are a reflection of their state of mind. For example, if an employee becomes disgruntled at being passed over for a promotion or begins to chafe under the new department manager's leadership style, that negative frame of mind will be evident in quantifiable changes in the language used in emails and instant messages. Also, if the person is seeking to migrate company data to personal devices clandestinely, he or she will suddenly start working late or coming in early, or will start to "show an interest" in documents and data which previously were passed over. UEBA actively profiles each user and compares real-time behavior and linguistics to the user's established baseline to look for anomalies which may indicate a growing possibility of unauthorized activities.

User Activity Monitoring provides real-time visibility into user actions without interfering in their productive activity. Then, for example, when an unintentional action potentially puts the company's data or digital assets at risk, the monitoring system can alert the proper response teams who can then mitigate the situation and inform the user what he or she did incorrectly. A balanced combination of UEBA and UAM will allow the organization to

ANALYZE
user activities and behavior patterns

DETECT
meaningful anomalies from established user norms that suggest genuine threats

PRIORITIZE
and focus their responses on the significant information

RESPOND
appropriately without putting undue stress on the organization's resources

Veriato Recon and **Veriato 360** integrate seamlessly to analyze and report insider behavior. Veriato Recon analyzes the users' psycholinguistics and activity, compares that behavior to recorded baselines, alerts when potential insider behavior is detected and keeps a rolling 30-day record on each local computer in a fully encrypted file of employee activity. Veriato 360 allows easy review of collected data through reports, a quick view panel dashboard, and video playback of activity screenshots. With Veriato's integrated solutions, organizations have the most comprehensive capacity to analyze, detect, prioritize, and respond to malicious and unintentional insider threats available today.

[i] Steinberg, Joseph. "Insider vs. Outsider Data Security Threats: What's the Greater Risk?" Nena Giandomenico, etal. Digital Guardian. Digital Guardian: Waltham. January 26, 2017.
https://digitalguardian.com/blog/insider-outsider-data-security-threats

[ii] Agarwal, Archie. "Meaningful Threat Modeling for CISOs." Peerlyst: San Francisco. March 17, 2017.
https://www.peerlyst.com/posts/meaningful-threat-modeling-for-cisos-anurag-agarwal

[iii] DeMille, David. "Will Your House be Broken into This Year?" A Secure Life: New York. March 2, 2017.
http://www.asecurelife.com/burglary-statistics/

[iv] Fleetwood, Blake. "Don't Let Terrorism Stop You from Visiting Orlando." The Huffington Post. The Huffington Post Media Group: New York. June 17, 2016.
http://www.huffingtonpost.com/blake-fleetwood/terrorism-tourism-and-orl_b_10512296.html

[v] "The Enemy Within Research." Clearswift: Theale. 2017.
http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf

[vi] Von Ogden, Jacquelne. "8 Examples of Interal-Caused Data Breaches." Cimcore, Inc: Merrillville. October 18, 2016.
http://blog.cimcor.com/8-examples-of-insider-internal-caused-data-breaches

[vii] "Venful EnerVest Operating Network Engineer Pleads Guilty to Intentionally Damaging Computer System." Office of Inadequate Security. DataBreaches.net. January 29, 2014.
https://www.databreaches.net/vengeful-enervest-operating-network-engineer-pleads-guilty-to-intentionally-damaging-computer-system/

[viii] Taylor, Ben. "Why there is a 1 in 3 Chance You'll get Hacked in 2016." BestVPN.com 4Choice, Ltd: Aldershot. March 2, 2016.
https://www.bestvpn.com/blog/43225/get-hacked-one-in-three/

[ix] "Insider Threat Spotlight Report." Veriato: Vero Beach. 2017.
https://www.veriato.com/docs/default-source/infographics/insider-threat-spotlight-report.pdf?sfvrsn=10

[x] "2016 Cost of Data Breach Study: Global Analysis." Ponemon Institute, LLC: Michigan. June 2016.
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

[xi] "2016 Cost of Insider Threats." Ponemon Institute, LLC: Michigan. September 2016.
https://dtexsystems.com/cost-of-insider-threat

Veriato
www.veriato.com

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410
+1 888 598 2788
sales@veriato.com

Veriato EMEA
3rd Floor,Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL United Kingdom
+44 (0) 1483 662888
sales@veriato.com

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/Veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/