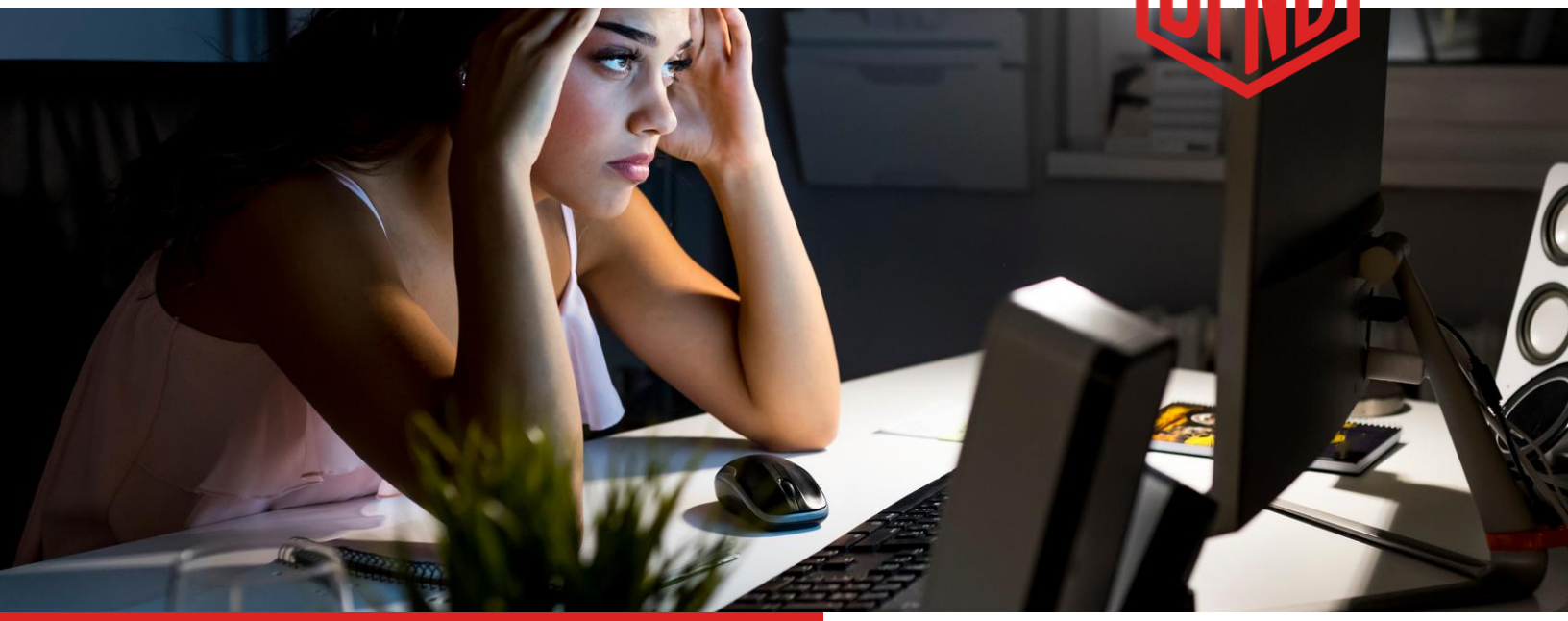
DFND SECURITY, INC.

AUGUST 26, 2020

PREPARING FOR INSIDER THREATS

DFNDSECURITY.COM



PREPARING FOR INSIDER THREATS DURING A PANDEMIC

BY GEOFF POER & ERIC HLUTKE

During this pandemic the question I get most is, "what is your biggest fear?". Without a doubt or hesitation my response is, “Insider Threats”. In hard economic times we see an increase in incidents that are perpetrated by insiders. The number one motivation for insider attacks is money. While we have all seen the recent ones in the news with Twitter, Tesla and Lockheed Martin, we have customers that have had insiders encrypt databases prior to a layoff and then demand money to unencrypt them.

Incidents sourced by trusted insiders are incredibly hard to detect and recover from. With tight budgets and projects being put on hold we wanted to spend some time on what you can do with little capital expenditure to be prepared and even prevent a major incident perpetrated by an insider.

"We aren't afraid of difficult problems, we like to call them 'Interesting Problems.'"

DFND Security has a 'Design for Impact' methodology that keeps us focused on the interesting problem, providing real impact to the organization and business. With the changes caused by the Pandemic, Insider Threats, being some of the hardest to detect, is our most interesting problem. They are conducted by users that may look like they are doing normal operational activities. False Positives can be damaging to morale and company culture. We need to reduce exposure without friction, increase detection and automate mitigation.

2.8M

The cost of Insider Threats (related to credential theft) for organizations in 2020 is $2.79 million.

2.5K

Businesses in the US encounter about 2,500 internal security breaches daily

47%

Over the last two years, the number of insider incidents has increased by 47%.

34%

More than 34% of businesses around the globe are affected by Insider Threats yearly.

WHERE DO WE START?

UNDERSTAND THE CHALLENGES

60% of major intrusions are due to trusted insiders with privileged access or knowledge. Many customers are planning to keep 30% or more of their employees at home indefinitely.

- The perimeter has grown and even moved into the home.
- Remote host remediation requires access and tools that may not currently exist in your environment.
- Incident Response workflows are often focused on external threats.
- Ability to monitor, identify and contain endpoints is limited, especially with new remote from home workers.

This is not a short term or circumstantial problem, that requires a long term solution.

EVALUATE YOUR SECURITY POSTURE

We often see companies spending more resources keeping the lights on, than they are in getting real value out of the solutions they have deployed. When evaluating your security program, keep these in mind:

- Don't put all your eggs into the compliance basket (ask Target).
- Understand your crown jewels and use your existing security investments wisely.
- Understand the asset and the incident response required for each of those assets.
- Monitor your security program's KPI's and metrics to ensure security controls are operating effectively and deviations are investigated thoroughly.

Focus on applying sound security discipline to protect what will cause the most harm.

FOCUS ON THE BASICS...

Detecting and preventing Insider Threats is even harder with increased WFH workforce and the expanding perimeter. Focus on your people and the processes with the technology you already have.

- Mature your Access Controls, especially Contractor and FTE on-boarding and off-boarding processes.
- Ensure your remote workers have DNS security capabilities.
- Mature your Identity and Privileged Access Mgmt (PAM), focusing on Privileged Account Credentials, Access Rights, Role Mgmt, etc.
- Evaluate data access rights based on roles and apply data security controls (ie: data masking, encryption, etc)

Do a quick Access Security Health Check.

- When was the last time the privileged account passwords were rotated?
- Do you have a list of the critical accounts? Often a list of all of the accounts does not exist. API keys are often overlooked.
- Do you have a trusted and tested method to rotate critical credentials? When was the last time these procedures were tested?
- If you have already invested in One Time Passwords for privileged access, how well is it monitored and backed up?

Avoid spreading FUD. Fear, uncertainty and Doubt detract from our ability to partner and drive real change.

- When addressing potential Insider Threats, use kid gloves and avoid looking like the security team just spreading FUD.

Ensure you have solid Back Ups.

- Identify and ensure all critical data has backed up and verified as working. Don't forget HR, payroll and user data (just ask Sony Pictures).
- Separate access controls from backups and database admins. Most Insider Threats are from single individuals.
- Use air gapped storage when possible.
- Make sure files are encrypted and protected. No one person should ever control the key.
- Restore Process Testing; when was the last time you tested the restore process?

Most companies don't collect and analyze the right data to detect Insider Threats, especially for lateral movement. Improve the monitoring of the data you have. Visibility is key.

- Ensure Mobile Device Management has achieved adoption on devices where company data is accessed.
- Logs that are stored only on local systems (usually app and database logs) can be changed and are the most vulnerable and volatile.
- Ensure data is centralized and in a secure location where it can be reviewed and analyzed.
- CASB and DLP tools require care and feeding to be effective. Monitor and update your rules.
- Find simple ways to control data leaving from BYOD and home networks.

Physical Security is critical with WFM. Facilities security should still have your attention even if staff are not coming into the office. Attacks can occur from empty offices on privileged networks.

- Monitor and investigate employee access to buildings if they are not considered essential.

"Train people well enough so they can leave, treat them well enough so they don't want to."
-Richard Branson

INSIDER THREAT WARNING SIGNS

- Major organization changes including layoffs and pay cuts.
- Morale dips or individuals that are actively talking badly about the company.
- Employees leaving (for any reason).
- Insiders accessing large amounts of data.
- Failed login attempts from legitimate accounts.
- Successful login attempts to outlier systems and services (why is this user accessing this service for the 1st time in... ever?).
- Alert for deletion of logs, disabling of logging services or logging source gaps.
- Alert for Anomalous Administrative tasks.
- Alert for Anomalous user logins to systems or services.
- New Hacking tools, Steganography tools, etc. showing up in the environment.
- Attempts to move data offsite.
- Key personnel experiencing:
  - Depression.
  - Stress in personal life.
  - Exploitable behavior traits; Use of alcohol or drugs, gambling.
  - Financial trouble.
  - Prior disciplinary issues.

PREVENTING INSIDER THREATS BY TREATING PEOPLE WELL.

- Treat your employees well. If you must do a layoff, pay for 6 months of insurance. If they have options, vest them (they will be less likely to want to cause harm to the company).
- Evaluate the possibility of bringing impacted employees back on a part time basis as contractors.

ENSURE YOU HAVE INCIDENT RESPONSE PLAYBOOKS FOR THESE COMMON INCIDENTS TYPES.

- Abuse of rights.
- Employee mistakes.
- Securing administrative access to cloud infrastructure.
- Malware account escalation and account takeover.
- Third-party access management.

66%

"66% of organizations consider malicious insider attacks or accidental breaches more likely than external attacks."

PARTNER WITH DFND, PROTECT AGAINST INSIDER THREATS

"Security strategy, implementation and operations is not only what we do best, it's what we believe in."

Hackers, Cybersecurity and Insider Threats are here to stay. Take control by allowing DFND Security to strategically architect iron-clad, custom solutions that will protect your business, confidential data, customers, infrastructure, and your users.

Contact us at sales@dfndsecurity.com.

Visit us online:

WWW.DFNDSECURITY.COM

WHY DFND?

Today's security threats require a comprehensive understanding of where your critical investments should be invested. DFND's approach allows you to make informed decisions to scale your Organization and Infrastructure on projects that deliver the most value for your investment.

Through meaningful partnership and a well thought out strategy we become an extension of your security team. Allowing you to focus on your businesses core competencies.

Scale your project team within days. Only work with the best people in the industry to innovate and execute for your business. We operate our technical recruiting arm with the idea that average is unacceptable. DFND's massive global network is backed by more than two-decades of technical recruiting experience.

As an extension of your security team, you will have better visibility into today's growing Cybersecurity threats and challenges. DFND's services enhance the effectiveness of your organization's capabilities by dealing with ongoing threats and defining policy to mitigate future attacks.

REFERENCES

- https://blog.paloaltonetworks.com/2013/12/the-cybersecurity-canon-the-cert-guide-to-insider-threats/
- https://blog.paloaltonetworks.com/2016/09/this-is-the-hardest-type-of-data-breach-to-discover-luckily-its-preventable/
- https://blog.paloaltonetworks.com/2020/01/cloud-ueba/
- https://adaptus.com/7-warning-signs-insider-threat/
- https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2
- https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf
- https://cdn.ttgtmedia.com/rms/security/InsiderTheft_ch03.pdf
- https://deloitte.wsj.com/cio/files/2016/04/2688954-Insider-Threat_4.pdf
- https://www.goalcast.com/2018/02/01/top-15-richard-branson-quotes/
- https://home.army.mil/bragg/application/files/3215/0515/6485/InsiderThreat.pdf
- https://us-cert.cisa.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat.pdfLockheed-martin-sold-employees-insider-threat-program
- https://techjury.net/blog/insider-threat-statistics/#:~:text=%20Coming%20up%20are%20some%20insider%20threat%20stats,breaches%20more%20likely%20than%20external%20attacks.%20More%20