Volume 3 • Issue 5

BLUF

BOTTOM LINE UP FRONT

the ThreatLab
Integrating Research Into Practice

Unintentional Insider Threat

The BLUF highlights what we at **The Threat Lab** are watching, listening to, reading, and thinking about. In this issue, we feature three artifacts that define unintentional insider threat, discuss its causes, and offer strategies on how to reduce such instances from happening.

PODCAST

From the OzCyber Unlocked podcast episode 14, Intentional or unintentional? The impact of insider threats, "One subject that often flies under the radar in the world of cyber security is insider threats…Some of today's most damaging security threats do not originate from malicious outsiders or malware, but from trusted insiders with access to sensitive data and systems…AustCyber's CEO Michelle Price speaks to Tracie Thompson (CEO and Co-Founder of HackHunter) and Dan Holman (CEO and Co-founder of WorldStack) about how human and technical threats are used to steal IP that is used in a variety of nefarious ways by cyber criminals."

Listen to the podcast
https://open.spotify.com/episode/5T1PxrIAZQhDDAALmbX436?si=mYhWcxejQM2C7ZfFkN6FAA

ARTICLE

From the article by Frank L. Greitzer, et al., Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies, "Organizations often suffer harm from individuals who bear them no malice but whose actions unintentionally expose the organizations to risk in some way. This paper examines initial findings from research on such cases, referred to as unintentional insider threat (UIT). The goal of this paper is to inform government and industry stakeholders about the problem and its possible causes and mitigation strategies. As an initial approach to addressing the problem, we developed an operational definition for UIT, reviewed research relevant to possible causes and contributing factors, and provided examples of UIT cases and their frequencies across several categories. We conclude the paper by discussing initial recommendations on mitigation strategies and countermeasures."

Read the article
https://ieeexplore.ieee.org/document/6758854

ARTICLE

From Susan Morrow's article, How to Create Awareness of Insider Threats, "Insider threats have a special place in the cybersecurity hall of shame. No one likes to think that their colleague is out to get them, but unfortunately, this type of threat to organizational security is all too real… Accidental insiders may not be malicious, but the harm they cause can be as bad."

Read the article
https://resources.infosecinstitute.com/topic/how-to-create-awareness-of-insider-threats/

The Defense Personnel and Security Research Center (PERSEREC) founded **The Threat Lab** in 2018 to incorporate the social and behavioral sciences into the mission space. The BLUF is made possible by the support of the National Insider Threat Task Force. To be added to our distribution list, please email **dodhra.ThreatLab@mail.mil.**