INSIDER RISK

PROBLEMS AND SOLUTIONS

A Sepio white paper

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

BACKGROUND

Advertisement

NEWS

Taiwan arrests BASF staff for selling secrets to China

Taiwan police have arrested at least six people for passing trade secrets to a Chinese company. Beijing has come under increased criticism for failing to stop intellectual property theft.

Wilders Security Forums

Police Warning [UK]: Cyber Criminals Are Using Cleaners to Hack Your Business

Discussion in 'other security issues & news' started by hawki, Feb 3, 2020.

BOINGBOING / XENI JARDIN / 2:53 PM TUE AUG 6, 2019

AT&T employees took over $1 million in bribes to plant malware and unlock millions of smartphones: DOJ

INTRODUCTION

For 90-95% of IT leaders the biggest cause of concern is humans and for 52% of businesses employees are their biggest weakness. According to a 2017 Kaspersky report, around 5% of all cybersecurity attacks were carried out by internal staff with malicious intent, with an additional 23% carried out by careless/uninformed employees. Although the majority of attacks come from outsiders this is still a large figure and it poses serious threats to organizations.

An organization might have the best software to secure their data center, the best physical security in and around the building, strong defensive technologies and the right security policies and processes in place, but should an employee act carelessly or maliciously, all these security measures are essentially useless.

Organizations are aware of the threat and have expressed concerns about it. This concern is not always linked to malicious attacks, but rather to inadvertent ones. Careless/uninformed staff can act in numerous ways that will lead to sensitive data and information becoming exposed. However, organizations also need to be aware of insiders who purposefully reveal confidential and sensitive information for personal gain.

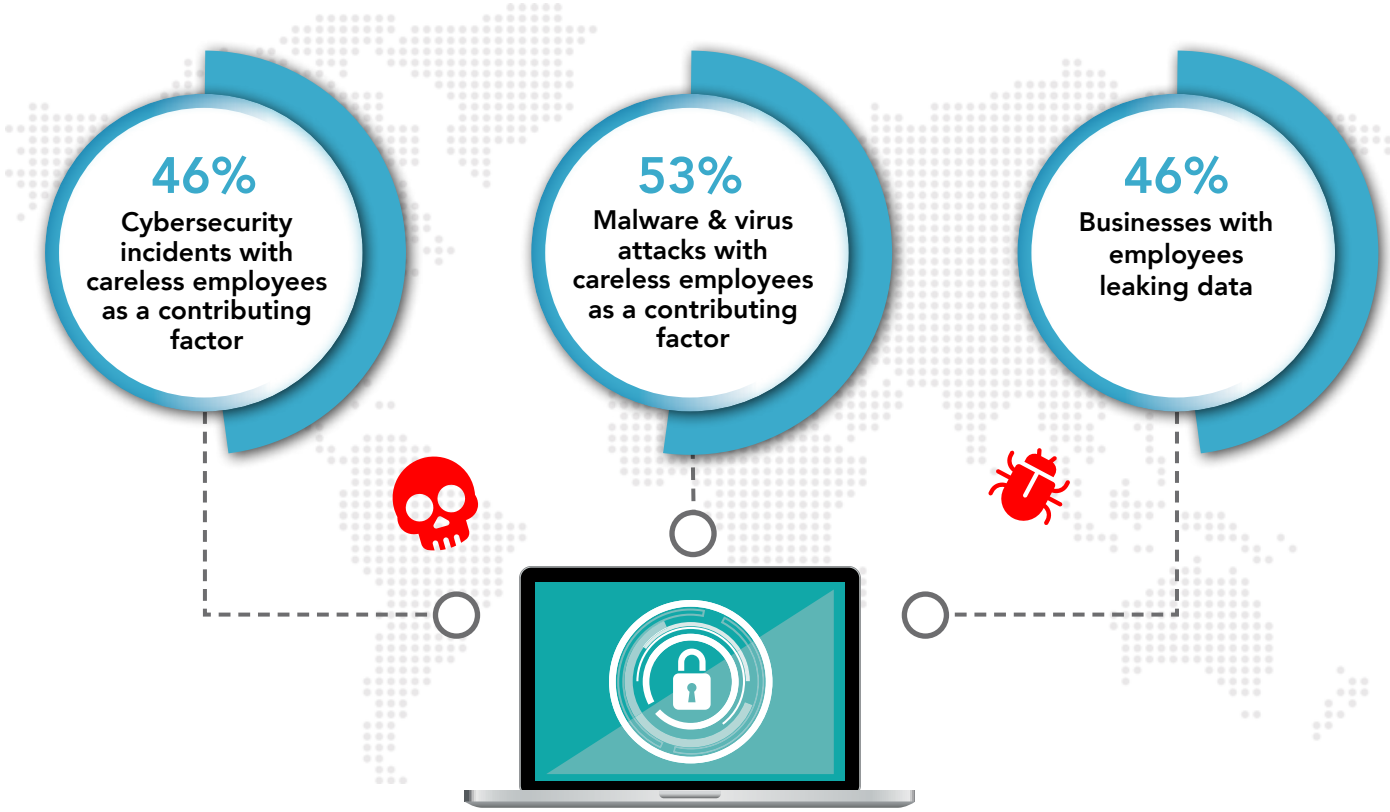
> ***"Around 5% of all cybersecurity attacks were carried out by internal staff with malicious intent."***

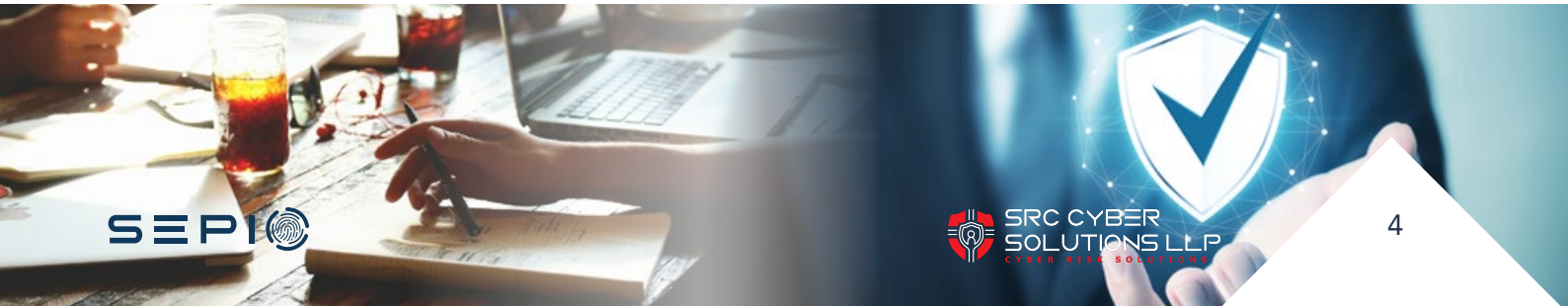
THREATS

STAFF ACTION

In 46% of cybersecurity incidents in 2016, careless employees have contributed to the attack. This is a large number considering that this is something that can be avoided, should staff be more diligent. Of the 49% of businesses that were attacked by viruses and malware in 2017, 53% of those incidents had careless/uninformed staff as a top contributing factor. Staff that are unaware of the sophisticated ways bad actors can carry out attacks makes them oblivious to the ways in which they can prevent them from occurring. Simply knowing about social engineering techniques such as phishing emails can help reduce the likelihood of a successful attack as staff are less susceptible to them. Likewise, augmenting employee awareness of rogue devices can encourage greater caution when using USB gadgets.

However, negligent employees also present a threat. 46% of businesses have irresponsible employees leaking/exposing data which is a great security risk for organizations.





In addition to leaking data, reckless employees have been found to lose sensitive or confidential customer/employee information (28%) and payment information (25%).

Furthermore, it was revealed that staff may hide an incident when it transpires. For 40% of businesses around the world this is the case. This might be for fear of being reprimanded, or because that employee believes that the problem will sort itself out/is not a grave threat. Whatever the reason, it is important for organizations to highlight the vitality of reporting an incident as soon as it appears in order to diminish the damage it can do in the long run. With employees hiding an incident, it means that management will only know about it when they need to know about it and, oftentimes, it will be too late.

EMPLOYER ACTION

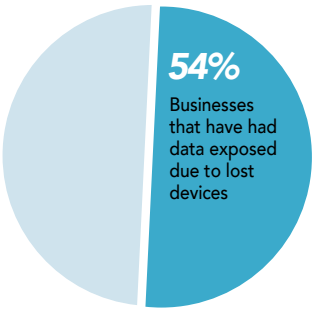
The reason for staff being uninformed may be down to the employer. Cybersecurity is important to all organizations and there are often measures enforced to ensure employees know this. However, overwhelming staff with rules and regulation can actually be the cause of their ignorance. Staff do not want to read extensive rules regarding cybersecurity; a topic that can be rather insipid. Even when staff do read them, it can be difficult to comprehend due to technical terminology. More exciting ways to inform staff of cybersecurity risks and protection measurements, such as interactive training days, will be of greater value to the organization as employees are more likely to be better informed.

BYOD AND IoT

Bring Your Own Device (BYOD) policies are being more frequently implemented among organizations and the rise of the Internet of Things (IoT) means that organizations face increasing threats from outsider devices.

Around 50% of businesses worldwide are concerned about employees inappropriately sharing company data via the devices they bring into work. Moreover, 54% of businesses have had data exposed because employees have lost devices that obtain sensitive information. Lost devices present a serious security risk. Hackers have no problem circumventing passwords and have even utilized rogue devices to bypass biometric authentication.

Personal devices tend to be less secure than those belonging to an organization, thereby being a prime target for perpetrators. Spoofed peripherals may act as a tool to carry out attacks and devices that operate outside of an organization are an easier target. For example, individuals frequently charge their phones at public charging kiosks; chances are, that mobile phone is also used for work purposes. As such, manipulating a charging kiosk is a way in which a bad actor can gain access to an organization's sensitive information without ever having to go near its premises. Thus, insiders that access the organization's network with their own device(s) put the security of the organization at risk if their device has been compromised. Organizations may require certain security measures to be enforced on personal devices, but this presents various complications including restricting user experience, and the cost incurred by organizations to implement these solutions, which is especially challenging for small businesses who may not have the budget for advanced security solutions such as NAC. Even if an organization does require specific security solutions to be employed on personal devices, when an employee leaves the organization they might disable the security feature. This is a problem if the company does not remove business data from an ex-employee's device. 60% of businesses do not do this, thereby having no control over that data when an employee leaves.



MALICIOUS ACTORS

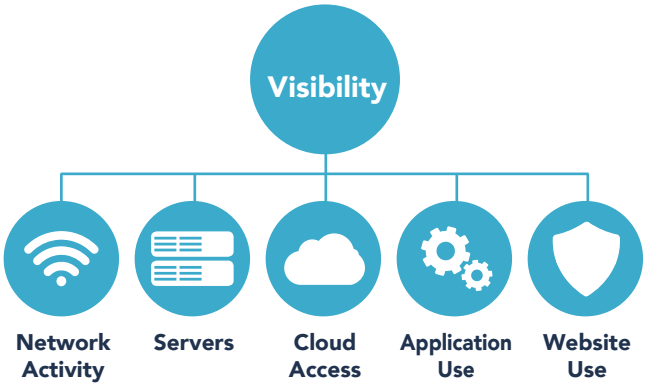
A dilemma organizations face is how to detect insiders who act with malicious intent. The aforementioned 5% of security breaches that were carried out by bad actors with insider access signifies a serious threat to organizations.

These individuals will purposefully act out against the organization and might employ rogue devices to carry out the attacks. Since these attacks occur on the Physical Layer (Layer 1), they are undetectable to software security solutions. Devices that appear genuine to the human eye, and to security software solutions, can exfiltrate information and/or inject malware onto the endpoint that can possibly spread throughout the network it is connected to.

Alternatively, insiders might be targeted by bad actors and socially engineered to knowingly carry out attacks. Although these insiders are acting against their will, there is malicious intent behind the attack.

SOLUTION

VISIBILITY



Visibility into network activity, servers, cloud access, and the use of applications and websites will provide organizations with insight into the actions of employees, indicating suspicious activity. This visibility must be comprehensive and span throughout the enterprise, both continuous and in real time. The security teams need to be able to see which user accessed which systems and files, and when, in order to detect and mitigate any risky actions. Furthermore, the tools should provide visibility outside the premises of the organization. More outsider devices being used means that organizations need to extent their visibility beyond their traditional walls.

INTELLIGENCE

With intelligence, security teams can make decisions based on actionable insights. Human behavior can be predicted with the help of analytics. This allows for the possible prediction of insider threats by detecting suspicious behavior which can then be further investigated.

RESPONSE AND REMEDIATION

Security teams need to be alerted about suspicious behavior as soon as it occurs in order to reduce the severity of the damage. Security tools should also provide mitigation for insider threats by automatically isolating and remediating user devices that are infected with malware to prevent the dissemination to other devices and systems.

Importantly, employees who access restricted websites put the organization at risk. These websites should be blocked by security teams to prevent staff from accessing them to avoid the unintentional installment of malware on devices.

HAC-1 SOLUTION

Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment.

This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement of hardware access. This may result in security accidents, such as ransomware attacks, data leakage, etc.

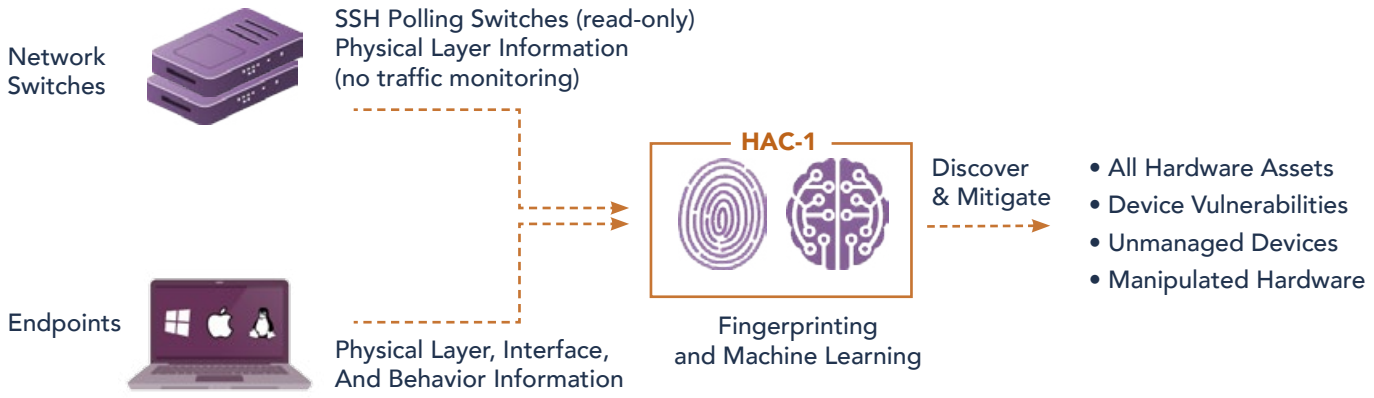
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, as well as take advantage of the "blind" spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce.

Sepio is the leader in the Rogue Device Mitigation (RDM) market and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. SepioPrime, which orchestrates Sepio's solution, identifies, detects and handles all peripherals; no device goes unmanaged.

The only company in the world to undertake Physical Layer fingerprinting, Sepio calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. With Machine Learning, the software analyses device behavior to identify abnormalities, such as a mouse acting as a keyboard.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

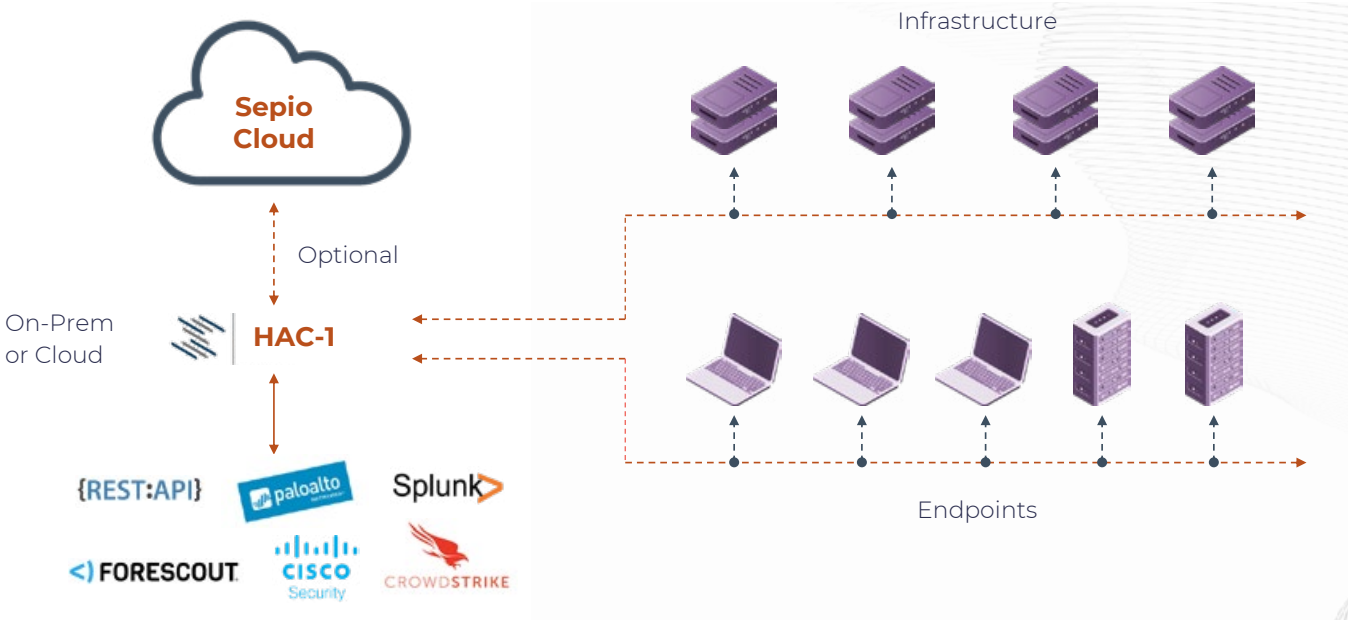
Main Benefits

Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

System Architecture



LEARN MORE

www.srccybersolutions.com +91 120 2320960 sales@srccybersolutions.com

ABOUT SEPIO

Founded in 2016 by cybersecurity industry experts, Sepio's Asset Risk Management (ARM) platform sees, assesses, and mitigates all known and shadow assets at any stage. The only trafficless solution, Sepio is infinitely scalable to protect the company's decentralized, uncontrolled ecosystem as fast and often as anyone, anywhere connects any assets. Sepio provides actionable visibility with the Asset Risk Factor (ARF) score based on a unique Asset DNA generated for each asset at its physical source, reflecting actual business, location, and rules. Sepio Radically improves the efficacy of NACs, EDRs, XDRs & Zero Trust layer solutions that simply see only the assets they are there to protect.
Visit: www.sepiocyber.com

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Highly Automated, and User-Friendly Solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection SEPIO for Asset Risk Management (ARM) to assess and mitigate all known and shadow assets at any scale, THREATX for WAAP (WAF ++) for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.