observe it

What the Trend Micro Breach Can Tell Us About the Insider Threat Problem

Even security firms like Trend Micro are vulnerable to Insider Threat problems. Sensitive data lives in many places and you can't just block employees interacting with it. Effective Insider Threat management can help defend organizations against this silent epidemic.

The last people you want to identify an Insider Threat breach are your customers. Unfortunately, that's what recently happened to security firm Trend Micro when a rogue employee sold information from a customer support database, according to the BBC. Allegedly, the firm learned about the incident only after customers complained of suspicious phone calls purporting to be from Trend Micro in August 2019.

Based on Trend Micro's investigation, it took them a month to conclusively prove an insider caused the breach. In this case, the sensitive customer data lived in the databases behind the commercial customer support portal and an employee seemingly accessed the database either by escalating their access privileges or bypassing existing controls. The malicious insider sold the customer information to third party scammers although the data exfiltration channels were not revealed.

When a security firm itself gets breached by insiders, it's solid proof that the Insider Threat problem can be a tough one to solve with traditional defenses alone. However, with an effective Insider Threat management strategy, organizations can often quickly and effectively identify these threats before they turn into an actual breach—and result in potential financial or reputational issues.

Decrease the Time to Discover an Insider Threat

According to cybersecurity expert Graham Cluley in the Trend Micro BBC article above, “You can have all the security in place to prevent external hackers getting in but that doesn’t stop internal staff from taking data and using it for nefarious purposes.” Many organizations make the mistake of focusing solely on external security, at the expense of Insider Threats. However, that approach could add up to a costly problem, if insiders are not effectively addressed.

Luckily, a dedicated Insider Threat Management solution is designed to help security teams quickly identify the root cause of an incident, by uncovering risky user activity and data movement. Tying it to the Trend Micro case, ObserveIT would monitor suspicious activity on servers and desktops, such as this customer support database and the employee’s desktop. More importantly, ObserveIT can detect the many malicious actions leading to the breach such as:

- Improper access of sensitive server (either by using shared accounts or somebody else’s identity)
- Download or copy of records from a database server
- Exfiltration through common channels such as email, web or cloud storage

Monitoring for a combination of user and data activity is important, because data doesn't move itself — people move data. A security analyst could identify suspicious activity in minutes within their SIEM or in the ObserveIT portal. In fact, many of our customers have said that ObserveIT enables them to spend minutes or hours on investigations that once took weeks or months. Deep user context allows organizations to quickly act on potential insider incidents (whether they're malicious or accidental).

Gain Context Into Potential Incidents

Unfortunately, many Insider Threat incidents can leave organizations guessing if they don't have the appropriate context into exactly what happened, from whom, when, and how. In Trend Micro's case, the scammers knew so much about customers that Trend Micro suspected its customer database had been breached. Rather than leave this type of information up to conjecture, organizations can know the whole story about Insider Threat incidents with detailed information on both user and data activity.

Using a solution like ObserveIT, security analysts can gain access to metadata onuser activity, file movement, and server activity that could be considered suspicious. In the example of unauthorized data exfiltration from a customer database, the system would trigger an alert that would inform the analyst about suspicious user activity. From there, the analyst would review the timeline of user activity and their movement of customer data before, during and after the ObserveIT alerts. The ObserveIT platform correlates activity across servers, web, applications and endpoints to the user in question so an analyst doesn't have to manually match up logs. For irrefutable evidence of wrongdoing, an analyst would pull screenshots of the user moving the data from the server and then exfiltrating from their endpoint. In highly regulated industries or countries, ObserveIT can anonymize user data for privacy and compliance purposes.