Uncovering data theft quickly

August 1 2017

Profile-based anomaly detection helps to uncover network attacks more quickly. Credit: Fraunhofer FKIE

Computer experts have always struggled to find solutions for protecting businesses and authorities from network breaches. This is because there are too many vague indicators of potential attacks. With PA-SIEM, IT managers have a solution that effectively protects their systems while exposing data thieves and criminal hackers more quickly than

conventional software.

When hackers targeted the German Parliament in 2015, it made headlines. The worrying thing about it was that the attack went undetected for a considerable period of time. In fact, it was only discovered by chance, by which time 16 gigabytes of data – consisting mainly of documents, e-mails and keyboard logs – had already landed in unauthorized hands. Cyberattacks like this one frequently hit authorities, businesses and other organizations. As an initial entry point, attackers often use phishing e-mails to gain access to the recipient's computer, or they infect websites regularly visited by the victim. As things stand, IT security experts can do little to prevent it. Although many organizations are collecting security-related event logs in their security information and event management (SIEM) systems, these systems also contain vast amounts of data about legitimate day-to-day operations, such as details of which users have logged in and logs of websites visited. It is simply not feasible for computer experts to fish out the alerts indicating a potential attack from this endless sea of data. In reality, SIEM systems often resemble data graveyards.

Detection and correlation of indicators from event logs

In the future, it will be possible to uncover network attacks more quickly. This is thanks to profile-based anomaly detection software for SIEM systems – PA-SIEM – which is being developed by researchers at the Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE in Bonn, who are collaborating with colleagues at OTH Regensburg and NETZWERK GmbH. The PA-SIEM project is funded by the German Federal Ministry of Education and Research BMBF. "Instead of relying only on predefined rules to detect cyberattacks, PA-SIEM calculates typical attack patterns from

incomplete or weak indicators," says Rafael Uetz, a scientist at FKIE. "This enables us to detect cyberattacks considerably more quickly and effectively."

The scientists are basing their work on a three-step process: First, the SIEM software gathers event logs from individual PCs and servers, as usual. Then, in the second step, special algorithms scan these logs for any anomalies or known threat indicators – essentially any deviations from standard behavior. The search results may indicate an attack, but not necessarily. Indications of an attack, for example, could be that a computer suddenly starts sending conspicuously large volumes of data to the internet. However, it could also simply be an employee sending unusually large files to a customer. Systems that detect such anomalies already exist, but they usually have a high false-positive rate. Even if this rate is only one per mille – meaning that one alert in every thousand is incorrectly identified as a threat – it can, depending on the size of the company, quickly set off several thousand false alarms in just one day.

Chains of events pave the road to success

"But it's essentially the third stage that makes the difference: we combine the indicators, which allows us to greatly reduce the error rate," explains Uetz. This can be demonstrated with a simplified numerical example: for an indicator that in 90 percent of cases is triggered by an attack, the false-positive rate would be ten percent. If two such indicators occur in close succession, say, if an e-mail comes in with a PDF attachment and then later the volume of data being sent to the internet spikes – this rate has already been reduced from ten percent to one percent. And if a third incident is then added to the chain, the false-positive rate is reduced again, now to just 0.1 percent. Incidentally, the German Parliament had fallen victim to a similar chain of events, which experts refer to as an "intrusion kill chain": The attackers first sent a spear-phishing e-mail to install malware, which in turn captured

passwords and administrator credentials, thus giving them all the information they needed to steal, delete and manipulate data. PA-SIEM software could have detected the whole incident much more quickly.

Provided by Fraunhofer-Gesellschaft