The Dangers Of The Darknet

AND WHY CONSTANT MONITORING OF WORKPLACE COMPUTER ACTIVITY IS A MODERN NECESSITY

Insights
11.01.16

Nearly every piece of data and information generated by businesses these days is corralled into various electronic storage sites, such as company network servers, software-as-a-service (SaaS) business applications, and cloud-based storage platforms. Despite the efficiencies that these electronic "safeholds" provide, employers are now examining how best to evaluate employees who have access to company technology systems and storage sites to ensure their company is protected from modern security threats.

As a practical matter, businesses are focused on operating and providing certain goods and services. Most employers pay attention to the needs of the day, and trust their employees to perform the tasks necessary to meet those needs. In this spirit, employers address employee deficiencies only when noticed, and management generally trusts that the workers will make good faith efforts to remediate the situation.

However, the days of sitting and waiting for poor performance before addressing employee behavior are about to become a thing of the past. Security threats posed by technology are now forcing companies to develop new approaches to systematically monitor employee performance and computer activity on a near-constant basis.

The Darknet: The Modern Digital Black Market

One reason businesses should maintain a state of perpetual vigilance is because of the ease with which unscrupulous individuals can profit from data breaches. In a recent article, investigative reporter Brian Krebs stated that fraud analysts have identified an increase in company inquiries regarding how best to handle disgruntled employees who are attempting to sell business data or network access on the "darknet."

The darknet refers to a hidden portion of the internet that you won't find by performing a standard Google search. Instead, users access the darknet through specific software, configurations, or authorization, often using non-standard communication protocols. They then access a specific IP address space configured in a manner that is not easily detectible. A major function of the darknet is to allow users to sell restricted goods, as the space allows peer-to-peer file sharing for illegal purposes.

Consider that there are forums on the darknet offering to target specific companies for phishing attacks. Members who have an axe to grind against an organization can post a bid and call on people to attack certain corporate targets, or offer to pay for another member to access certain corporate databases. Some forums even solicit names of potential "insiders" who might easily be recruited or extorted by unsavory characters.

Why is this important to consider? Because now employees need not be technically sophisticated computer hackers to pose a threat. Instead, they only need to have access to a company's network or data and either harbor a grudge or be susceptible to threats or extortion by an outsider looking to gain online entry. Essentially, this can be any worker with a computer.

Daily Monitoring Is More Important Than Ever

Given that insider breaches are generally undetected until significant damage occurs or is looming, each company must rethink their approach to evaluating workers and create corresponding objective measures. In other words, more than end product or function-based assessment is required.

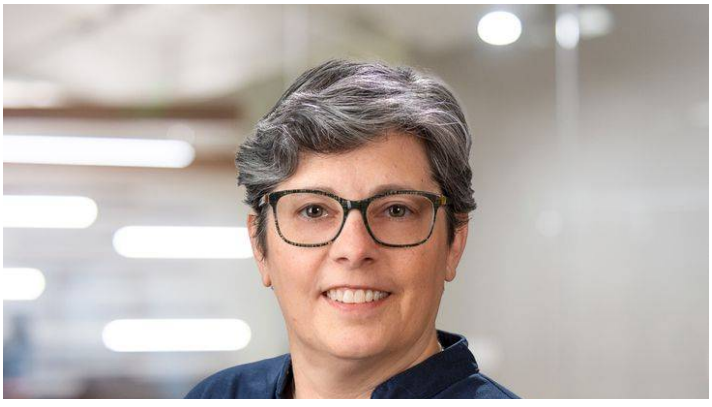
You should make regular and ongoing assessments of how employees access and use networks, data, and intellectual property to minimize the threat of the insider to the greatest extent possible.

If you invest in the development of systematic monitoring and evaluation of employees, you will better position your company against operational interruptions, monetary expenses, and other consequences of an "insider" selling network access or data.

Keeping a pulse on workers and incentivizing them to report threats can mean the difference between staying in business and unexpectedly closing your doors. Best practices require that you similarly monitor your systems and implement accountability measures for any other individual or business with access to your networks or data, including contractors, consultants, and gig workers.

For more information, contact the author at SMoore@fisherphillips.com or 440.740.2132.

Related People



Sarah Moore
Of Counsel
440.740.2145
Email

Service Focus

Privacy and Cyber

Counseling and Advice