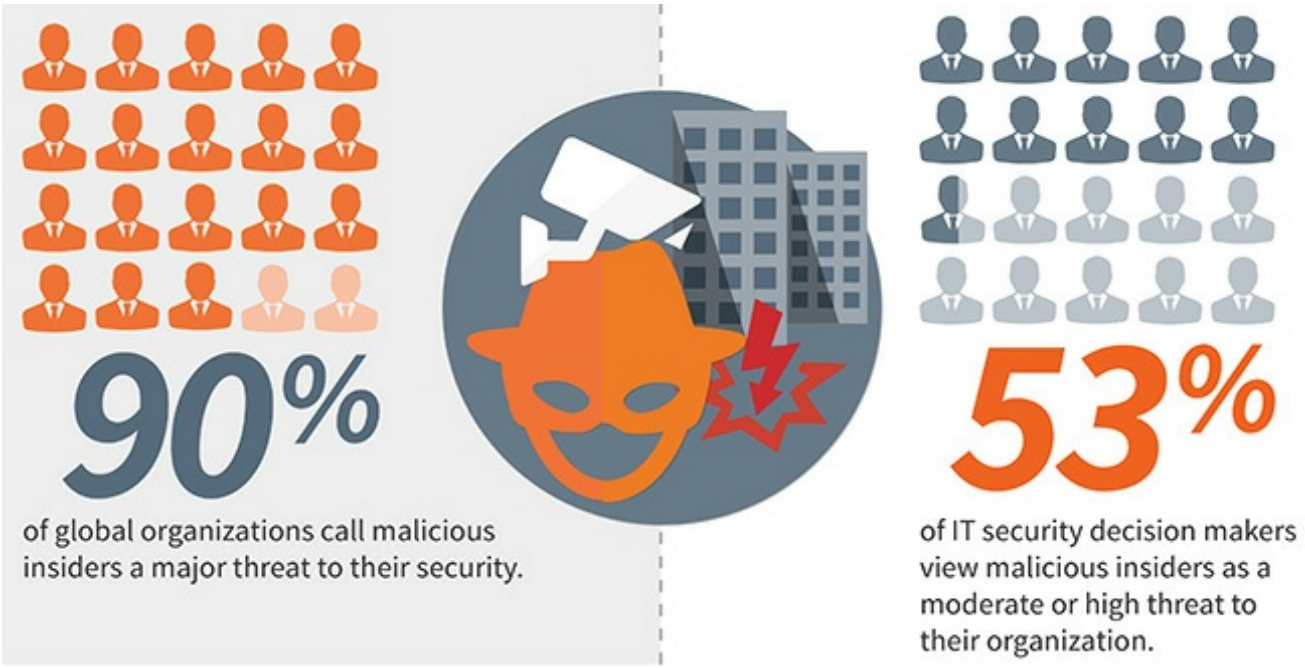
Organizations still unprepared for malicious insiders

helpnetsecurity.com/2016/08/17/malicious-insiders/

Mirko Zorz 8/17/2016

Organizations globally believe they are their own worst enemy when it comes to cybersecurity, with 45 percent saying they are ill-equipped to cope with the threat of malicious insiders and twice as many, 90 percent, calling malicious insiders a major threat to the organizations' security, according to Mimecast.



"Companies' IT security priorities usually change depending on different factors, among which the budget and the threat vectors are the most important for most. If last week Oracle's POS breach was the most debated, most surely retailers using POS devices and all organizations working with financial data have started to check their own systems and to see how they can strengthen their security for that specific threat. In the light of such incidents, insiders threats are left out, so it is no wonder that 45 percent are ill-equipped to cope with malicious insiders," Roman Foeckl, CEO at CoSoSys, told Help Net Security.

"It is also realistic that 90 percent of organizations see malicious insiders a major threat, but I would include here also negligent insiders. From our encounters with CSOs from organizations in different verticals, we noticed their fear is directed towards insiders in general, not necessarily malicious ones. In case of human error, there is the risk of people uploading sensitive files on unsanctioned applications, copying confidential information on cloud file sharing apps or making print screens of critical data and publishing it on unauthorized online services. Regardless if we're talking about malicious or careless employees, to prevent data losses or thefts, businesses should define what data should be allowed or not to be transferred and through what channels, if it's e-mail, instant messaging, cloud file sharing apps, or portable storage devices," explains Foeckl.

Is your email security up to par?

Mimecast uncovered that 65 percent of IT security decision makers globally feel their email security systems are inadequately equipped to handle cyber threats.

By concentrating predominately on perimeter defense and outside threats, organizations around the world struggle with the risk that comes from their own people, emphasizing the need for organizations to implement employee awareness and education as well as creating a cyber resilience strategy that includes both technology- and human-based defenses. This is evident especially considering this study revealed that nearly half of the organizations polled felt exposed to malicious insider attacks.

The research also uncovered that:

- Over half (53 percent) of IT security decision makers view malicious insiders as a moderate or high threat to their organization.
- One in seven IT security decision makers view malicious insiders as their number one threat.
- Those who say they're very equipped on cybersecurity feel virtually just as vulnerable to insider threats as those who believe they aren't equipped at all (16 percent vs. 17 percent), indicating that the risk of malicious insiders trumps perceptions of security confidence.

"It's no surprise that even the most cyber-ready companies are terrified of insider threats. It was always possible for employees to steal or misplace valuable corporate data, but never this easy. Cloud services have facilitated the movement of data into and out of the enterprise like never before – which is both a great asset and risk to businesses," says Andreas Zengel, EMEA CTO at Skyhigh Networks.

"Cloud services have vastly expanded the scope of insider threat. The most common insider threat scenarios – such as a salesperson jumping ship, rogue sys admins or simply employees committing security missteps in the process of doing their job – are all enabled by cloud computing, and much more difficult to detect due to the nature of modern business operations. With the vast amount of interactions with cloud services by each user every day, it is essential that enterprises put in controls and intelligent monitoring solutions that can filter out the noise of day-to-day usage from the activities performed by a malicious insider and pro-actively warn security operations and prevent actions when an anomaly or threat was detected," Zengel concluded.

Mimecast tips for safeguarding against malicious insiders

1. Assign role-based permissions to administrators to better control access to key systems and limit the ability of a malicious insider to act.

2. Implement internal safeguards and data exfiltration control to detect and mitigate the risk of malicious insiders when they do strike, to cut off their ability to send confidential data outside the network.

3. Offer creative employee security training programs that deter potential malicious insiders in the first place and help others to spot the signs so they can report inappropriate activity to their managers. Then, back that up with effective processes to police and act swiftly in the event of an attack.

4. Nurture a culture of communication within teams to help employees watch out for each other and step in when someone seems like they've become disenchanted or are at risk of turning against the company.

5. Train your organization's leadership to communicate with employees to ensure open communication and awareness.