Insider attacks are becoming more and more popular and difficult to detect

Internal attacks are becoming more and more popular in recent years.

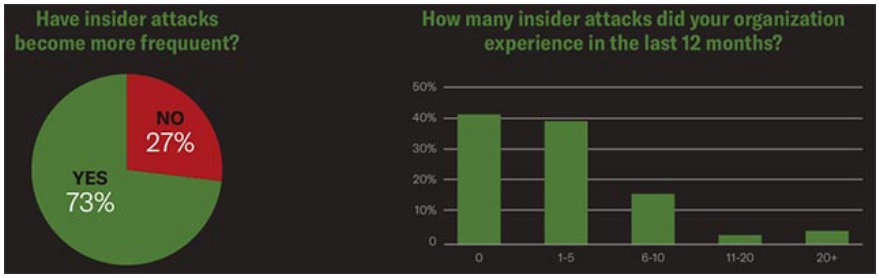
Perhaps just hearing through the name, we can somehow imagine that this form of cyber attack is directly related to people working in the targeted network, for example. As a certain IT (IT) employee feels "dissatisfied" with his boss, he decides to "knock down" the network of the company where he is working. Attacks on the internal network can be harmful or harmless depending on the purpose and level of the attacker. Typically, internal attacks often involve acts such as deliberately eavesdropping, stealing or destroying information, fraudulently using information or unauthorized access to an important data warehouse.

1. [Infographic] How to recognize and prevent Phishing attacks

Internal attacks are becoming more and more popular in recent years. According to Bitglass, 73% of the surveyed IT experts said that their companies often face internal attacks. While 59% were asked to declare that the systems they managed also experienced at least one incident involving internal attacks in the past 2018.

Cloud Access Security Brokerage Company (CASB) Bitlass has obtained these results after conducting a large-scale survey with the participation of 437 IT professionals, and cooperating with Cybersecurity community. Insiders includes more than 400,000 other information security experts worldwide.

While in reality, most organizations and businesses are aware of the dangers from the threats initiated by malicious agents outside their systems, Bitglass also recognizes that there are quite a large proportion of organizations, this business absolutely does not notice that it is equally important to make countermeasures to discover and prevent the threat of insider attacks. .



1. New ransomware detection not only encrypts files but also helps 'clean up' the system

The fact that 68% of IT professionals surveyed said that their organizations are in the range from moderate to extremely vulnerable to threats from inside is evidence of the importance of It is extremely urgent for all organizations and businesses to build and establish defensive security measures to deal with internal attacks.

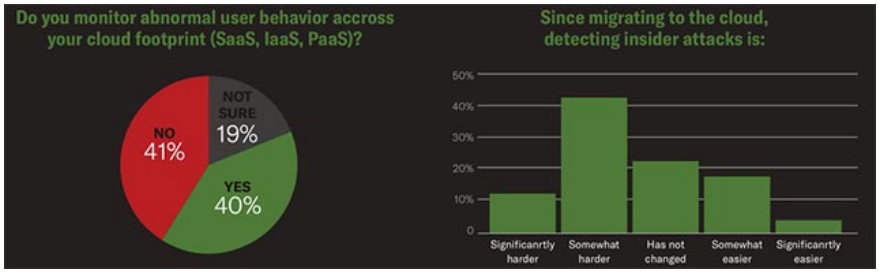
"In fact, internal attacks are often more difficult to identify and fix than external attacks. This is because internal attacks are often caused. by a number of factors existing in many network systems, including inadequate authentication capabilities, inadequate user behavior monitoring on cloud platforms, and lack of proper security settings for devices If individuals want to prevent internal attacks, they must first solve the problems mentioned above, 'said Rich Campagna, CMO of Bitglass.

In general, internal attacks are often particularly dangerous because they are more difficult to detect than attacks coming from outside sources, because of the fact that internal security controls in the corporate network careers are often less respected, and this contributes to the conditions for 'insiders' to attack the system they are working on.

1. The alarming increase in the number of attacks targeted at IoT devices

Besides, the problem got worse when reporting on Bitglass's internal threat in 2019 also found that "only 50% of the surveyed organizations provide security training. for users and their employees about possible threats to the internal system, and only 31% implement secondary authentication to protect their systems. '

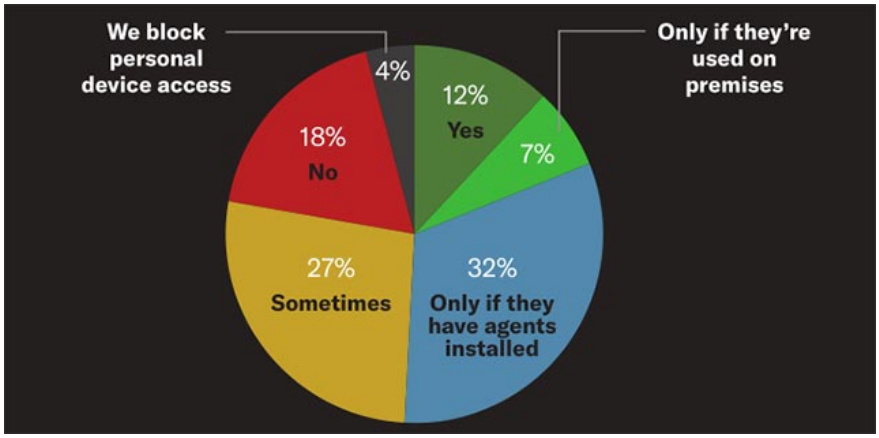
In addition, 56% of the experts interviewed said that internal threats were often detected in their organizations during the day, while 50% stated that the recovery of the consequences after the attack was also will be done and completed at the end of the day after the attack.



1. Endpoint Detection and Response threats, an emerging security technology

41% of respondents said that Cloud migration is considered one of the leading factors making internal attacks even more difficult to detect and combat, especially When many organizations and businesses do not implement appropriate tools to monitor "unusual behavior of users on the cloud platform".

On the other hand, 56% of IT professionals interviewed by Bitglass claim that internal threats will become harder to detect when an organization moves its IT infrastructure to the cloud, as well as move between multiple cloud platforms.



1. What is cybercrime? How to prevent cybercrime?

In addition, when asked by Bitglass whether his company can detect internal threats stemming from personal mobile devices, only 12% of respondents said they are currently own the tools and knowledge needed to do that.

The final and equally important data, that is, 56% of endpoint devices in general, and 46% of mobile devices in particular are the 2 most commonly used devices in launching attacks. internal work.