Corporate security prediction 2020

kaspersky

CORPORATE SECURITY PREDICTIONS 2020

The popularity of cloud services is growing, and threat actors are here to exploit the trend.

We are observing more and more cases where our customers' infrastructure is partially or entirely located in the cloud – cloud migration has been the dominant trend of the past couple of years. This is resulting in a blurring of infrastructure boundaries. In 2020, we expect the following trends to emerge:

- It will become more difficult for attackers to separate the resources of the targeted company from those of cloud providers. It will be much more difficult for companies to detect an attack on their resources in the initial stages.

The transition to the cloud has blurred the boundaries of company infrastructures. As a result, it is becoming very difficult to target an organization's resources in a precise manner. So, conducting an attack will become harder and the actions of threat actors will become more sophisticated or more frequent – relying on chance rather than planning. On the other hand, it will also be difficult for a company to identify targeted attacks at an early stage and separate them from the overall mass of attacks on the ISP.

- Investigating incidents will become more complex and in some cases less effective.

Those who plan to deploy cloud infrastructure in 2020 need to talk in advance with their provider about a communications plan in the event of an incident, because time is of the essence when it comes to security incidents. It's very important to discuss what data is logged, and how to back it up. Lack of clarity on such information can lead to complications or even make successful incident investigation impossible. We note, however, that awareness of cloud infrastructure security is not growing as fast as the the popularity of cloud services, so we expect to see an increase in the complexities of investigating incidents as well as a decrease in the effectiveness of incident response.

It's also worth noting that when companies pass on their data to a cloud provider for storage or processing, they also need to consider whether the provider possesses the necessary level of cybersecurity. Even then, it is hard to be absolutely certain that the services they are paying for are really secure, as it requires a level of expertise in information security that not all technical officers possess.

There is a number of ways such insiders can be recruited:

- By simply posting an offer on forums and offering a reward for certain information.
- The attackers may disguise their actions so that employees don't realize they are acting illegally, disclosing personal information or engaging in insider activity. For example, the potential victims may be offered a simple job on the side to provide information, while being reassured that the data is not sensitive, though it may in fact relate to the amount of funds in a bank client's personal account or the phone number of an intended target.
- Blackmailing. We also expect to see increased demand for the services of groups engaged in corporate cyber-blackmail and, as a consequence, an increase in their activity.

- Criminals will migrate to the cloud and forge ahead.

The increase in the availability of cloud services will allow not just companies but also attackers to deploy infrastructure in the cloud. This will reduce the complexity of an attack and, consequently, will increase their number and frequency. This could potentially affect the reputation of the cloud services themselves, as their resources will be used in large-scale malicious activity. To avoid this, providers will have to consider reviewing their security procedures and change their service policies and infrastructure.

Insiders market is expanding

The good news is that we are observing an increase in the overall level of security of businesses and organizations. In this regard, direct attacks on infrastructure (for example, penetrating the external perimeter through the exploitation of vulnerabilities) is becoming much more expensive, requiring more and more skills and time for the attacker. As a result, we predict:

- Growth in the number of attacks using social engineering methods.

In particular, this means phishing attacks on company employees. As the human factor remains a weak link in security, the focus on social engineering will increase as other types of attacks become more difficult to carry out.

- Growth of the insider market.

Due to the increasing cost of other attack vectors, attackers will be willing to offer large amounts of money to insiders. The price for insiders varies from region to region and depends on the target's position in the company, the company itself, its local rating, the type and complexity of insider service that is requested, the type of data that is exfiltrated and the level of security at the company.

Cyber-blackmailing groups that collect compromising info on company employees (e.g. evidence of crimes, personal records and personal data such as sexual preferences) for the purpose of blackmail will become more active too in the corporate sector. Usually this happens in the following way: the threat actors take a pool of leaked emails and passwords, find those that are of interest to them and exfiltrate compromising data that is later used for blackmail or cyberespionage. The stronger the cultural specifics and regional regulations, the faster and more effective the attackers' leverage is. As a result, attacks on users in order to obtain compromising data are predicted to increase.