May 5, 2022
More information: press@nordlayer.com

The 5 most common cybersecurity mistakes and the ways to avoid them

Against steadily increasing cyberattacks, companies should embrace holistic solutions rather than temporary ones

The population of the internet has reached 5 billion users. Every day, 250 thousand new websites are added to the current 1.17 billion active websites. Online retail accounts for 3.5 trillion USD in revenue. The more the internet ecosystem expands, the more deeply companies are connected to global technology networks. As businesses grow more dependent on the internet, cyberattackers are becoming more sophisticated and adaptable to defenses. About 450 thousand new malicious pieces of software are created each day. Nearly 2,000 data breaches and over 300 million ransomware attacks happen each year.

In the face of novel and constant attacks, a shift of focus appears from destructive malware to spyware and data retrieval. And companies pay a heavy price for the steadily increasing number of cyberattacks. Although awareness about cyberattacks has increased in recent years, the types of cybersecurity mistakes made by corporations have not changed much. According to Juta Gurinaviciute, the chief technology officer at NordLayer, here are the 5 most common cybersecurity mistakes companies still make and ways to avoid them:

1. Using outdated network models

Traditional network models that have a single entry and exit points are based on a simplified design, and basic encryption models are still in use by many small and middle-sized companies. Traditional networks' lack of AV software, their inability to be easily scalable, and their lack of segmentation are enough to make the business open to a cyberattack. In modern networks, local networks are segmented by function. This makes them easily scalable and more reliable in terms of security. Using modern network standards based on fully virtualized WAN, zero-trust network access frameworks, and SASE makes remote networks more resilient and less prone to high-level cyberattacks.

2. Relying on anti-virus solutions

In today's sophisticated threat landscape in which a shift of focus appears from destructive malware to spyware and data retrieval, relying solely on anti-virus technologies is not enough to fight against cyber attackers. Anti-virus only helps protect against known viruses, and cyber attackers strive to create new and sophisticated methods every day. Traditional anti-virus solutions may catch common malware but are no match for advanced adversaries with stealthy intrusion tactics. Implementing a multi-layered network security approach effectively protects your technology environment. It is also a robust solution for slowing down attackers.

3. Opting for on-premise solutions rather than cloud-based

Although on-premise software solutions allow companies to maintain a level of control, they require in-house server hardware, software licenses, integration capabilities, and IT employees on hand to support and manage potential issues. In contrast to an on-premise environment, in a cloud environment, companies have access to those resources that are hosted on the premises of the service provider and use as much as they want at any given time, scaling up or down depending on overall usage. Besides, in contrast to on-premise systems offering much less data security, cloud solutions do not involve many physical and virtual components that act as potential malware entry points. They offer much better security and do not require users to constantly manage and monitor security protocols.

4. Inability to do capacity planning

While companies maximize business opportunities, they continue to focus on day-to-day solutions such as buying limited licensed protections or setting up hardware solutions with physical limitations when it comes to cybersecurity. And they disregard planning for the future. To avoid limited solutions, they should do detailed capacity planning by forecasting the needs of IT based on historical trends and infrastructure metrics. Capacity planning and transforming infrastructure align with business objectives because growth is considered. User increase is one of the main steps to ensure IT resources are sufficient to meet future needs.

5. Settling for minimum solutions rather than secure the full infrastructure

Securing infrastructure with minimum effort such as installing a firewall but not having a fallback or installing an antivirus but not an intrusion detection system only creates a

temporary solution. Cybersecurity requires a holistic organizational approach more than ever. Therefore, companies should follow best practices and implement a cybersecurity framework like SASE that offers businesses comprehensive security through shielded visibility, data protection, and increased edge-to-edge security for the network perimeter — and all devices within it. By combining software-defined edge networking, user-centric authentication, access control, and seamless integration across the cloud, SASE is a blueprint for better business security.

Istock image

ABOUT NORDLAYER

NordLayer is an adaptive network access security solution for modern businesses — formerly NordVPN Teams; NordLayer helps organizations of all sizes to fulfill scaling and integration challenges when building a modern secure remote access solution. Moving towards an ever-evolving SASE framework, NordLayer's solutions are quick and easy to implement with existing infrastructure, hardware-free, and designed with ease of scale in mind. NordLayer meets the varying growth pace and ad-hoc cybersecurity requirements of agile businesses and distributed workforces today. For more information: nordlayer.com.