EINPRESSWIRE

Business’ Data Privacy Under Concern With Record Internet Traffic in 2021

The three pillars of company data protection: people, process and technology

UNITED STATES, January 29, 2021 /EINPresswire.com/ -- According to Cisco, this year the daily internet traffic will reach [7.7 exabytes]() — the equivalent of 7.7 billion GB or 1.9 billion DVDs, and a 50% increase compared to 2020. Growing volume of information might increase the chance of a data breach: global losses from cybercrime exceeded $1 trillion in the last year.

Some call our increasing reliance on data a ‘fourth industrial revolution’, but to reap its rewards enterprises have to also think about robust protection of their corporate perimeters. As virtual data becomes one of the most valuable resources, officials are in the process of setting up fair rules of the game.

> Today data protection stands on three pillars: people, process and technology. Organizations have to invest in them accordingly to build a robust cybersecurity perimeter.”
>
> *Juta Gurinaviciute, CTO at NordVPN Teams*

“When it comes to data breaches, companies tend to think that they won’t attract hackers’ attention. However, the lessons of remote working show that people are prone to human error, and the cybercriminals don’t adhere to any rules. They do not discriminate between manufacturing, medical, financial and other sectors, and target all of them,“ says Juta Gurinaviciute, the CTO at [NordVPN Teams](). “With strict rules being set by the legislators, enterprises are no longer responsible for their own intelligence, but their clients’ and contractors’ data as well”.

Data protection is everyone’s job

According to an Avast survey, 70% of employees in an organizations think the biggest cybersecurity threats lay outside their company. However, 88% of data breaches are caused by human error, either by them falling victim to social engineering or not complying to cybersecurity playbooks.

The other side of the coin is that only 43% of workers admit having compromised their corporate network. Their silence should be attributed to the fear of consequences, as 40% of employees are afraid that they will be held personally responsible for a data breach. This keeps them from informing the other parties about the risk.

“A resilient organization is built on trust and employees shouldn’t be afraid to inform the security teams about the incident. Enterprises can also mitigate the risk by implementing zero trust network access (ZTNA) solutions. With them, users can only access the information needed for their functions, and only for a time needed to complete the job,” advises Gurinaviciute.

The question of cybersecurity will transcend the corridors of IT and security departments, and everyone within the organization will be in charge of protecting the data. Half of the CISOs told PwC that they plan to incorporate privacy into all business decisions, so they’ll require everyone’s dedication.

“Every team in the organization relies on data: manufacturers share the know-how, marketers know everything about their customers, sales keep the secrets about profit margins, and people from finance make dozens of millions-worth transfers each day. Given the tremendous internet traffic, the security team is unable to closely monitor everything—a conscientious workforce is the best way to stay protected,” says NordVPN Teams’ CTO.

Protecting your company’s data

Whilst every employee in the organization is responsible for its cybersecurity, the burden of arming them with the appropriate protection falls on the security officers. However, 74% of organizations stunningly admit that their cybersecurity plans are either ad-hoc or inconsistent, or they have no plans at all.

“It is crucial to organize a business' data before setting up a cyberattack emergency plan. In order to implement effective security measures, enterprises must map out and classify the information, ranking it from the most to the least sensitive,” says the NordVPN Teams’ expert.

Encryption also adds an extra security layer to the classified information. It scrambles the data into the unreadable sequence of bits, and only those with permission can decrypt it. This method and thorough privilege management reduces the surface area for cyberattack. However, go easy on protection tools, as their effectiveness gradually falls when using 50 or more of them.

“Today data protection stands on three pillars: people, process and technology. Organizations have to invest in them accordingly to build a robust cybersecurity perimeter without vulnerabilities or weak spots. Experts have to think about securing their data in the cloud, especially when Cybercrime-as-a-Service no longer requires programming skills to profit illicitly," says Gurinaviciute.

Auste Valikonyte
NordVPN Teams
email us here
Visit us on social media:
LinkedIn