Acronis issues warning of critical privacy risks in 2021 ahead of Data Privacy Day

As incidents of brute force attacks skyrocket and 80% of companies operate without password policies, experts warn that breaches in 2021 to expose more data

Acronis issues warning ahead of Data Privacy Day 2021

DUBAI, UNITED ARAB EMIRATES, January 28, 2021 /EINPresswire.com/ -- Acronis, a global leader in cyber protection, today issued a warning that, based on their research of recent cyberattack trends and existing business practices, organizations around the world currently face a global threat to data privacy and security. The company announced its findings on international Data Privacy Day to alert organizations that immediate action is needed to avoid costly attacks.

The latest research by the cybersecurity experts at the global network of Acronis Cyber Protection Operations Centers (CPOCs) revealed that 80% of companies do not have an established password policy. Between 15-20% of the passwords used in a business environment include the name of the company, making them easier to compromise. Two recent high-profile breaches illustrate this problem: Before its Orion compromise, SolarWinds was warned that one of its update servers had a publicly known password of "solarwinds123", while former President Donald Trump's Twitter account was hacked because the password was allegedly "maga2020!".

Of the organizations that do have a password policy in place, the researchers found many rely on default passwords – and up to 50% of those are categorized as weak.

Attackers know these weak password practices are widespread and, with so many employees working from home as a result of the COVID-19 pandemic, cybercriminals have targeted the less secure systems of these remote workers. Acronis analysts observed a dramatic increase in the number of brute force attacks during 2020 and found that password stuffing was the second most used cyberattack last year, just behind phishing.

“The sudden rush to remote work during the pandemic accelerated the adoption of cloud-based solutions,” explains Candid Wüest, VP of Cyber Protection Research at Acronis. “In making that transition, however, many companies didn’t keep their cybersecurity and data protection requirements properly in focus. Now, those companies are realizing that ensuring data privacy is a crucial part of a holistic cyber protection strategy – one that incorporates cybersecurity and data protection – and they need to enact stronger safeguards for remote workers.”

Financial and reputational risks
While the business community is recognizing that better cyber protection is needed to ensure the privacy of their data and their customers’ data, awareness among digital users continues to lag. One report found that 48% of employees admit they are less likely to follow safe data practices when working from home.

Poor password hygiene and lax cybersecurity habits of remote workers are among the reasons Acronis CPOC analysts expect the financial impact of data exfiltration will soar in 2021, as bad actors can more easily access and steal valuable company data. The trend is similar to one now seen among ransomware attackers, who are stealing proprietary or embarrassing data and then threatening to publish it if the victim doesn’t pay. Last year, Acronis identified more than 1,000 companies around the world that experienced a data leak following a ransomware attack.

Implementing tighter authentication requirements
To avoid the costly downtime, significant reputational damage in the marketplace, and steep regulatory fines that can be caused by a data breach, organizations must strengthen the authentication requirements needed to access company data.

Acronis and other cybersecurity experts recommend the following best practices:
- Multifactor authentication (MFA), which requires users to complete two or more verification methods to access a company network, system, or VPN, should be the standard for all organizations. By combining passwords with an additional verification method, such as a fingerprint scan or randomized PIN from a mobile app, the organization is still protected if an attacker guesses or breaks a user’s password.
- Zero trust model should be adopted to ensure data security and privacy. All users, whether they are working remotely or operating inside the corporate network, are required to authenticate themselves, prove their authorization, and continuously validate their security to access and use company data and systems.
- User and entity behavior analytics, or UEBA, helps automate an organization’s protection. By monitoring the normal activity of users with AI and statistical analysis, the system can recognize behavior that deviates from normal patterns – particularly those that indicate a breach has occurred and data theft is underway.

While Data Privacy Day 2021 is an ideal opportunity to bring attention to the risks to data privacy, the researchers at the Acronis CPOCs have identified additional cyberthreat trends that will challenge sysadmins, managed service providers (MSPs), and cybersecurity professionals

during the coming year.

The full analysis is currently available in the recently released Acronis Cyberthreats Report.

Melwyn Abrahams
Matrix Consulting
043430888
email us here
