A $ 1,000,000 MISTAKE:

How to protect the company from risks when employees work remotely.

FUDO SECURITY

For effective teamwork, it is not necessary for everyone to be in the same office. The principle of remote work was first tested by the world's leading companies. For example, back in 2018, Jack Dorsey, the head of Twitter, suggested that his employees try working from home. A bold experiment at that time showed excellent results: **the team's work efficiency increased.** **Since March 2020, Twitter has rented out some of its offices, and the principle of remote work has become an element of the company's corporate culture.**

The COVID-19 pandemic has accelerated the transition of various companies (especially in the IT field) to a remote or partially remote work system for employees. In a pandemic, this approach allows you to reduce risks for the company, take care of employees, and reduce operating costs for maintaining offices.

DID YOU KNOW...

A poll by consulting firm Gartner shows that many large companies are determined to leave workers at home after the pandemic, writes American Forbes. Analysts surveyed 317 CFOs at companies with annual revenues ranging from $ 500 million to $ 50 billion and employing up to 100,000 people. **75% of them approved the idea of transferring part of their employees to remote work.** Furthermore, the data tells us that 17% of top-level directors plan to keep 20% of their staff in remote work environments. Also noteworthy is that 4% of managers would like to have 50% of their staff working from home[1].

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations--to-shift-some-employees-to-remote-work-permanently2

However, this approach also contains huge risks that company executives cannot ignore.

Top management of Twitter has identified two main problems of „remote work”:

Gaps in the security of the connection to the company’s network.

Analysis of the productivity of employees.

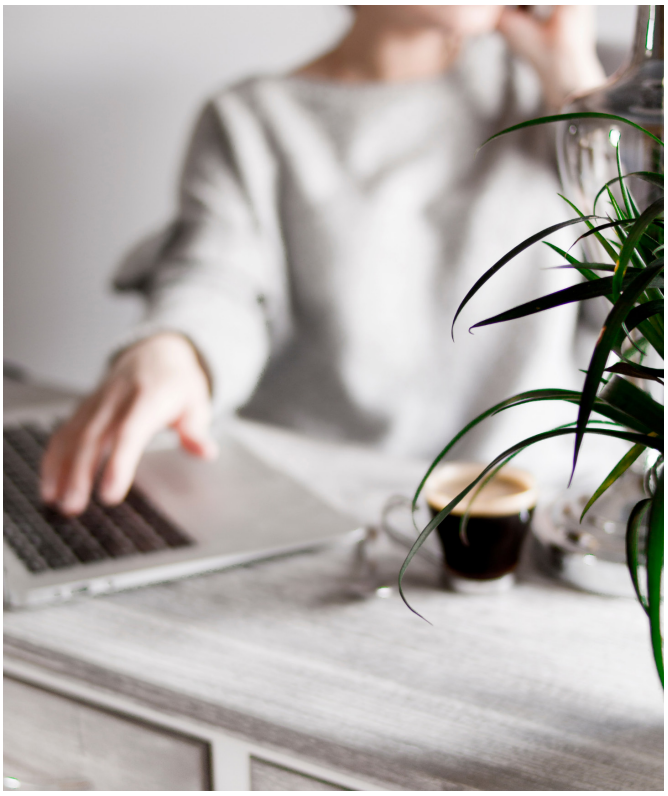
July 15, 2020 became a real „black” day for Twitter. The microblogging service plunged 3.2% after major trading. **The main reason is a hacker attack,** which affected the accounts of the largest businessmen, celebrities and corporate accounts of large companies. For example, from the accounts of Obama and Elon Musk, followers began to receive messages with an appeal to send them bitcoins. Twitter employees were automatically logged out of their accounts, and many were unable to log in to chat with colleagues or try to resolve the situation.

A serious blow to the company’s reputation and profits, isn’t it? How could this happen in such a large and seemingly reliably protected company?

The hackers used a massive attack using social engineering techniques. For example, when a letter comes allegedly from a manager with a request to provide certain information. If you are in the office, it is easier to check with your boss what he meant. However, when an employee works from home, when he has an unsecured Internet connection, and there are pets and children around, then vigilance is dulled. **This is actively used by cybercriminals.**

For many companies, the transition to work in „home offices" was a surprise. It was not possible to properly ensure the required level of information security when employees work remotely.

As a result, most of today's remote access systems in a company are a hardware or software solution on the company side and a VPN client on the user side. These can be both commercial products and free ones, for example, OpenVPN. In this case, home or personal computers and laptops are used as a workstation. And this is all the protection of remote connections!



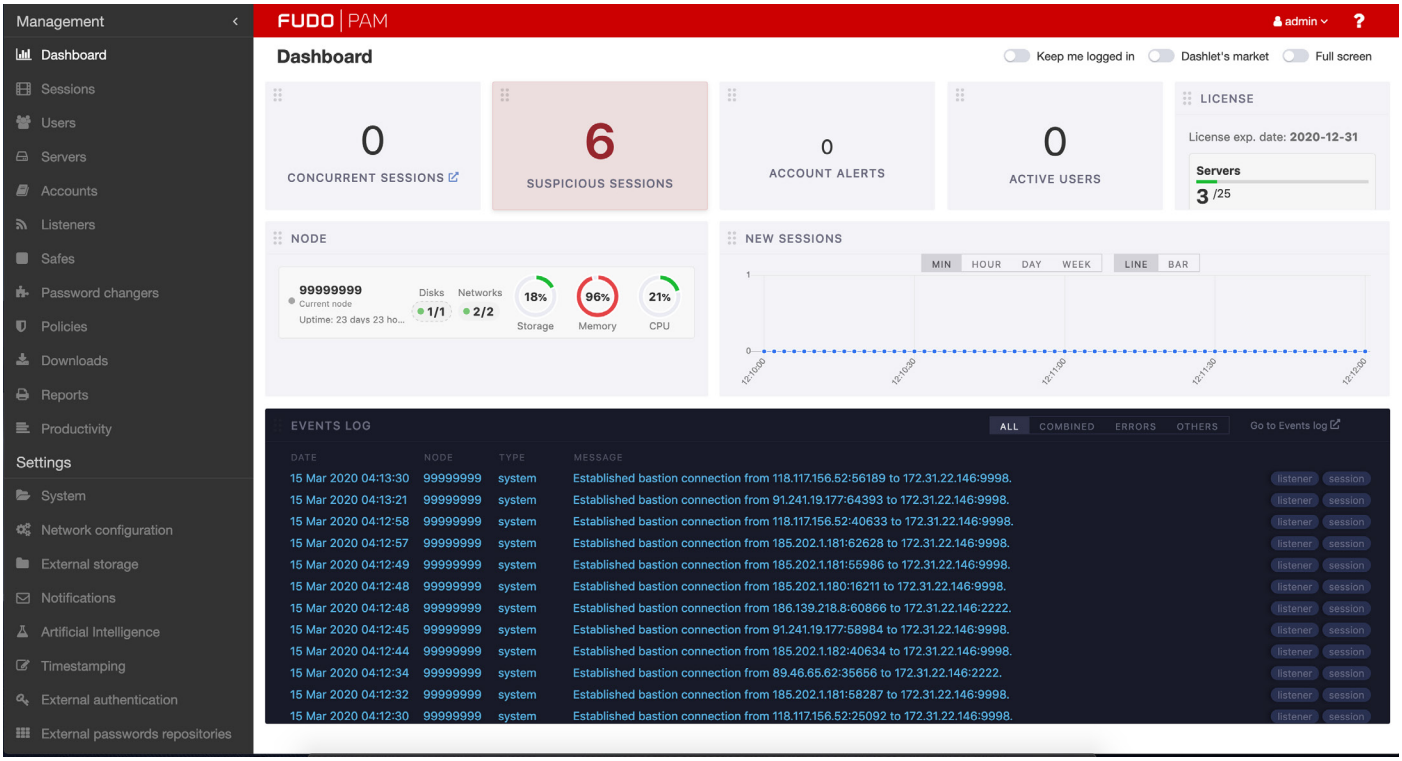
Naturally, such weak protection led to a sharp increase in incidents and an increase in the number of hacks.

Over the past six months, the number of cyberattacks has increased by 150%.

Over the past six months, the number of cyberattacks has increased by 150%. For example, if at the beginning of the year the number of attacks on the „remote desktop" was slightly less than **60,000 per day** around the world, then during the pandemic, the number of attacks was - **more than 100,000 per day!**[2]

This is a challenge for both company executives and information security departments. It is necessary to choose a solution that will provide reliable protection against cyber fraudsters, and at the same time, implementation will not take much time and will be financially affordable.

2 https://www.esetnod32.ru/company/press/center/eset-vo--vtorom-kvartale-kolichestvo-atak-na-rdp-vyroslo-v-dva-raza/



Fudo PAM is a ready-made hardware or software solution that is deployed on the customer's network within 2-3 hours without requiring the purchase of any additional licenses.

As security for the remote connection, Fudo PAM offers the client the inclusion of an additional, **2nd factor of authentication.** For example, it can be a code generated on your phone by the free Google Authenticator app. The user enters his username and password, and then the code is given to him by the application.

Thus, even if a hacker stole a user's login password, without access to his phone he will not be able to connect to the company's resources.

This feature is free for Fudo PAM users and supports both the free Google Authenticator and Microsoft Authenticator apps, as well as commercial products like Vasco, RSA, Cisco DUO, and others.

Certainly, corporate systems of user account Microsoft Active Directory and LDAP are supported. In this case, it is possible to combine access from corporate systems with various methods of two-factor authentication. **There is no need to install any software on users' servers and workstations.**

To provide an assessment of the performance of remote employees, which is so important for the business, Fudo PAM includes the **Efficiency Analyzer module.** This module analyzes the activity of an employee within a remote session: **the activity of using the mouse and keyboard, the amount of information displayed on the screen.**

If a detailed analysis or "debriefing" is required, remote sessions can be recorded as a video file.

This information is collected, analyzed by the Fudo system. Then, in the form of graphs and reports, it is presented to the business: reports by departments, groups, personally by an employee. **If a detailed analysis or "debriefing" is required, remote sessions can be recorded as a video file.** You can always view a controversial situation.

At the same time, it should be noted that the recording is carried out only within the framework of the working session, so if an employee uses a home computer for work, the privacy of his life does not suffer.

As a welcome addition for security personnel, there is an opportunity to further enhance protection. the Fudo system includes biometric analysis, like a digital handwriting, to further protect the user from a stolen credential misuse.

Thanks to this function, the Fudo system allows you to warn a security employee or even block access automatically if someone else uses the employee's password. An outsider's handwriting will be different from that of a real employee.

All of these features allow companies of any level to quickly add essential controls to their remote employee access system. **This will enhance security and allow the business to monitor the performance of its employees.**
It is worth noting the ease of implementation of the Fudo product. Fudo Security offers unique and customized pricing models to make it affordable to every situation. It allows you not to worry about the number of users - it is not limited. For example, connecting 100 users to 1 server requires the purchase of only 1 Fudo license. And all of the above systems will be included in this license.

Alexander Tvaradze

Business Development Manager

fudosecurity.com

Secure Remote Access

Deployable in a single day.

US: +1 (408) 320 0980
EMEA: +48 22 100 67 00
DACH: +49 911 - 30 91 80

sales@fudosecurity.com

FUDO SECURITY