Few Security Solutions That Can Boost Your Protection

Too many warnings create a burden on IT employees. Cybersecurity professionals need to implement better ways to filter, prioritize, and correlate incidents.

Increase security and ignore warnings

No security solution will provide you with 100% protection from existing and new, increasingly complex threats. There are two basic problems with IT security. The first is the constant growth in the number and complexity of cyber threats, which is an objective problem and cannot be much influenced.

Another problem that can be influenced is mistakes and misperception of the situation. Companies make mistakes when it comes to some simple operations, which makes the company vulnerable to various attacks. Although there is no single solution or approach to full protection, there are simple things that need to be done to increase the level of security and to provide the conditions to defend against growing threats. So, if you try to avoid the mistakes in question, you will significantly raise the level of security.

Too many warnings create a burden on IT employees. Cybersecurity professionals need to implement better ways to filter, prioritize, and correlate incidents. They need to use a single platform to collect data, identify cyber threats, and monitor dismissals. It is a concept of active response to threats where the point is in immediate response, not just in identifying threats.

Picture 1 of Few Security Solutions That Can Boost Your Protection

Grant admin privileges

Administrative privileges are what every hacker strives for because in that way they can cause great damage to the company. Most users do not need to be given admin privileges to perform normal activities. Exposure to threats is significantly reduced if a restriction is established in the introduction of new applications that require users to admin credentials. Thus, security analysts are left with a digital footprint that helps them quickly identify problems, especially those that indicate a security breach or intrusion into the system.

At each approval of administrator rights, the IT department should perform an appropriate risk analysis. IT managers must assess the possible damage in case of compromising user accounts and what kind of impact admin rights will have on secondary systems. The admin approach must be the exception, not the norm. If applied appropriately, organizations can proactively identify problems instead of spending weekends cleaning up compromised systems.

Many organizations ignore it when employees use social networks and cloud services on their own. However, the potential for the IT crisis is quietly simmering as internal business users create their own IT infrastructure that is not in line with corporate policies. Cloud application connection control can increase visibility when using unauthorized software and can limit the risk of losing intellectual property or sensitive information.

Unpreparedness for loss

There is a risk that an employee will accidentally forget an official laptop or smartphone somewhere and never find it again. This risk is even greater if the employee is often on a business trip. If the device is encrypted and can be accessed from a remote location, this is not a significant problem. However, if there are unprotected sensitive documents in the device, this is a cause for alarm.

IT administrators need to know what data is stored in which places. In the case of sensitive data, care must be taken to ensure that the devices are protected (encrypted) and that some of the remote access tools (such as VPNs) that can (and must) be disabled are lost.

With the evolution of cyber threats comes progress in incident management. What, unfortunately, does not change is the fact that people must constantly be reminded of how important it is to take care of "small" and often boring, repetitive IT practices because ignoring them endangers the security of the organization. Things like forgetting to revoke admin privileges to the user and giving access to "third party" printers can be fixed and brought under control. With a responsible approach, IT professionals put their company in the best possible position when it comes to dealing with existing and new threats.

Password managers as an answer to several problems

Internet passwords must be long, complex, and ideally, we must have a separate password for every account on the web. It complicates our digital life. But some tricks will help. Cancel passwords - for several Internet users, this may be the correct solution. But it isn't that easy. The mix of username and password is the most typical method of logging on to numerous social networks, shopping portals, or forums on the web.

Many users make things easier for hackers by applying passwords that don't seem to be. Thus, "12345678" and "password" are still among the foremost popular passwords. This has its reason because many ask themselves: how am I able to even remember such a lot of different passwords? But it's also possible - with technical assistance.

Picture 2 of Few Security Solutions That Can Boost Your Protection

Here are the most effective methods and their advantages. Password-manager remembers all our passwords and loads them when the necessity arises. On the pc, the login data is usually ready. Good password management programs also are ready to come up with passwords that are very difficult to crack.

We must trust within the company that sold us the password manager, that is, we must be convinced that the memorization and transmission of passwords are finished consistent with ok standards. Password managers, like Keeper, also allow us to attach to other devices, use two-factor authentication likewise as automatically fill in various queries and files. Use them and be safe and secure. Some of our own or others' activities on the Internet may endanger our security. On the Internet, our privacy and reputation can be endangered, our money in bank accounts can be robbed, our computer can be disabled.

Even personal and family safety can be compromised if we behave carelessly online. The computer we use for surfing and similar activities must have a program to identify and destroy viruses that could harm our computer and the data on it. There are sites and content on the Internet where we can easily infect our computer, but also experience some inconvenience or be deceived.