CYBERSECURITY: IDENTIFYING THE WEAKEST LINK

The majority of organizations implement a cloud strategy in order to be more efficient or save capital investment costs. But there is one advantage that many organizations overlook: the cloud can enhance (data) security. Surely sensitive data stored elsewhere might sound threatening, but a reliable cloud provider or reputable cloud service should have the appropriate licenses, expertise and hard- and software to secure sensitive data to a maximum. A cloud provider is better prepared for attacks, data leakage or even power cuts than any of us in the life sciences industry can prepare for.

DATA SECURITY THREATS

There are several cloud service models one can choose from: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) or Infrastructure-as-a-Service (IaaS). Whether or not the selected solution actually uses, stores and processes sensitive data, it might form a security threat to your IT systems. Whether sensitive data is stored on-premise or in the cloud, there is one thing you can be certain of: cybercriminals can find a way to access it by for example;

- Installing Malicious Software (Malware) - Malware is unwanted software that is placed on your network. Once inside the network, the malware uses a vulnerability in software being used by the organization and damages or disrupts a computer, laptop, server or mobile device. These days, one of the biggest threats to data is ransomware. This type of malware aims to block access to systems or encrypts your data (cryptoware). After paying ransom, the blockage is removed.
- Targeting employees via email (spear phising) - Most attacks on corporate networks have their origin in an attack on one of your employees (social engineering). By contacting them via email and seducing them to click on a link or open an attachment, cybercriminals install malware on your employee's device. Once the device connects with the organization's network, the cyber criminal can gain access to sensitive data.
- Looking at software - Whether it's cloud based software or if it's installed in a secure private network, cybercriminals can always find a backdoor in software. Often the cybercriminal spots these weaknesses - and is able to gain access to sensitive data - well before the software devel oper is aware of the defect.

The impact of a cyber attack stretches much further than financial damage. In addition, it creates chaos, stolen data is sold to a competitor and the reputation of the life sciences industry is at risk.

TAKING MEASURES AGAINST CYBERRIME

There are several things you can do to protect your systems against many types of cybercrime. By educating employees on spear phising, the number of infected computers should reduce. Furthermore, backups will reduce the impact of ransomware and regular software updates prevent cybercriminals from accessing your systems. Other measures include encryption of your data before saving it to your servers and choosing extra access login measurements like two factor authentication. Taking the right security measures is however time consuming and needs constant attention due to the ever evolving threat landscape. Therefore, an increasing amount of companies in the life sciences industry adopt a cloud strategy to strengthen effectiveness of their cybersecurity policy.

CYBERSECURITY: IDENTIFYING THE WEAKEST LINK

SECURITY BY CHOOSING THE CLOUD

Data loss, hacks and viruses: years of research shouldn't get lost or compromised. With the unstoppable number of digital innovations, going at it alone is not advisable. Organizations that have outsourced their IT find the right partner in a certified cloud provider. Especially when the cloud provider of your choice specialises in life sciences by providing industry standard certified infrastructures, platforms or software solutions.

It's important to monitor which incidents threaten your network. Since a cloud provider manages more than one network, it has insight into different types of threats and has a good understanding of when and where these pop up. This information is used to compose an incident response plan based on life sciences industry standards.

A data center - the location where your IT infrastructure, software solutions or data is stored - physically safeguards your servers by providing emergency facilities such as fire extinguishers and generators in case of a power cut. These type of security measurements are costly and are far stretched from your IT department's daily work.

RELY ON AN EXTRA SET OF EARS AND EYES

By identifying the weakest link in your data security, it becomes clear that in many cases human beings are the main threat to our systems. Think about it, mistakes are being made while developing software and employees are unaware of installing malware. Therefore an extra set of ears and eyes that safeguards sensitive data is not a luxury, it's become a necessity.