techconsult
TECHNOLOGY MARKET ANALYSTS

CYBER SECURITY REIMAGINED!

HOW NEW CONCEPTS SUCH AS ZERO TRUST OR SASE ARE TRANSFORMING EXISTING SECURITY CONCEPTS

In collaboration with

LANCOM SYSTEMS

Information about the study

This study was created by

techconsult
TECHNOLOGY MARKET ANALYSTS

Contact

techconsult GmbH
Mail: info@techconsult.de
Phone: +49 561 8109 0
Fax: +49 561 8109 101
Web: www.techconsult.de

Publication date

04/2022

In collaboration with

LANCOM SYSTEMS

Other Information

This study uses gender-neutral language wherever possible. All terms, examples and information therein applies generally to all genders in the sense of equal treatment.

Inhaltsverzeichnis

Introduction

Cyberattacks are omnipresent and constitute a huge threat to the entire economy, regardless of size or industry. The rapid increase in mobile work and cloud services is also making companies even more vulnerable to cyberattacks. While greater flexibility is achieved through remote work and cloud services, the new structures, at the same time, create new attack vectors for cybercriminals which should sound the alarm bells with IT security experts. The spread of shadow IT and the integration of new sites also continue to increase the risks.

Prominent examples from 2021 show that cyberattacks are becoming as dangerous as never before. For example, retail giants MediaMarkt and Saturn were the victims of a large ransomware attack at the end the year – with huge consequences. Cash registers and merchandise management systems had been encrypted by the ransomware, the workflows were severely disrupted and the cybercriminals demanded a ransom of 50 million dollars. This is just one of many examples where cybercriminals have been able to circumvent the defences in order to cause damage. In addition, the number of cyberattacks will continue to rise exorbitantly in the future. According to Check Point Software's 2022 Security Report, the number of attacks on company networks in 2021 compared with the previous year increased by 62 percent in Germany, by 117 percent in Austria and by 65 percent in Switzerland .

At the same time, cybercriminals are becoming more and more sophisticated and are increasingly able to bypass conventional IT security infrastructure. This is because, in the age of digitisation, with a huge increase in data traffic by more and more devices and subscribers, these old, static structures are no longer up to date. Companies need to change the way they think and adopt new security concepts that extend beyond their company network and ensure that IT security is maintained.

Two of these key concepts are the Zero Trust approach and secure access service edge (SASE). Zero Trust is a security concept in which generally all devices, users or services are mistrusted from the outset, without making any difference whether the service, the device or the user is located inside or outside the in-house network. In conventional security concepts, everything that is inside is considered trustworthy. SASE is understood as a cloud architecture model that bundles network and security-as-a-service functions into a common cloud service. This includes firewalls, secure web gateways and also network access according to the Zero Trust principle.

The results of this study show to what extent German companies are making use of cloud services and what measures they take to ensure that access to cloud services from private terminals is secure. In additions, the companies surveyed provided information on how often they have been affected by cyberattacks, what consequences this had for them, which means they use to fight cyberattacks and what the degree of maturity of their implementation of Zero Trust and SASE concepts is.

Source:
https://www.ict-channel.com/security/letztes-jahr-62-prozent-mehr-cyberangriffe.126621.html

If you want to read the whole document, you can get the complete techconsult PDF free of charge via our **contact form**.

LANCOM SYSTEMS