

10

claranet®



Cybersecurity Trends that your organization must follow in the next months

Todos os dias novas ameaças de cibersegurança colocam em risco utilizadores individuais e organizações de todas as dimensões.

48%

Foi o aumento anual de ciberataques baseados na Cloud registado em 2022. ¹

61%

Percentagem de crescimento dos ataques de phishing no mesmo ano. ²

8

trilhões

Custo, em dólares, que o cibercrime deverá provocar em 2023. ³

Dez tendências a seguir para aplicar medidas de segurança mais robustas e adotar a legislação adequada aos novos tempos.

1 - Soluções Cloud-based

A mudança para a Cloud traz novos desafios de cibersegurança. Invista em soluções de proteção focadas nos desafios introduzidos por estas plataformas.

2 - Inteligência Artificial na Cibersegurança

A adoção generalizada de soluções de segurança alimentadas por Inteligência Artificial permitirá detetar e prevenir ciberataques em tempo real.

3 - Segurança da IoT

O crescimento da adoção de dispositivos associados à Internet das Coisas (IoT) - que incluem desde termostatos inteligentes, a câmaras de segurança - obriga a um foco maior na sua proteção contra ciberataques.

4 - Proteção de dados

Cada vez mais informação pessoal e sensível é armazenada pelas organizações, tornando essencial mais investimento em novas soluções e protocolos para uma proteção responsável dos dados.

5 - Phishing mais sofisticado

Os ataques de phishing continuam a ser uma grande ameaça para organizações e indivíduos, sendo de esperar um aumento na sofisticação destes ataques.

6 - Aumento do Ransomware

É de esperar, em 2023, a continuidade da tendência de aumento registada nos outros anos. A formação dos utilizadores e a proteção de todo o perímetro de IT das organizações são essenciais para enfrentar este perigo.

7 - Supply chain attacks

As organizações terão de estar especialmente vigilantes ao seu ecossistema de fornecedores, uma vez que estes tipos de ataques são de difícil deteção. Será de esperar a adoção acelerada de soluções VRM (Vendor Risk Management).

8 - Zero Trust

Este modelo de segurança garante que todo o tráfego de rede é tratado como potencialmente malicioso. Desta forma, as organizações podem adequar a segurança das suas redes, sobretudo em modelos de trabalho híbridos.

9 - Soluções de MDR e XDR

A integração de soluções MDR (Managed Detection and Response) e XDR (Extended Detection and Response) com serviços de SOC aumenta a eficiência e a eficácia na deteção e resposta a incidentes de segurança.

10 - Ambiente regulatório complexo

Regulamentos como o NIS2, DORA e DL n.º 65/2021 do GDPR exigem o cumprimento de requisitos rigorosos de proteção e segurança de dados. Isto requer uma abordagem holística e contínua de cibersegurança, incluindo a formação de funcionários e a monitorização contínua.

2023 está a moldar-se para ser um **ano desafiante no mundo da cibersegurança** e os próximos meses poderão ser decisivos para muitas organizações. Acompanhar as últimas tendências, implementar medidas de segurança robustas e estar em conformidade com a legislação constituem práticas a adotar... o quanto antes!

¹ dados Check Point Research

² The State of Phishing 2022

³ eSentire 2022 Official Cybercrime Report

claranet®

helping our customers do amazing things