Cyber Attacks – Best Practices for HR Leaders

Cyber attacks have become a major threat to businesses, leading to financial losses, damage to reputation, and disruption of operations. Understanding their impact is crucial for implementing effective response measures.

By Daniela Mertens

1

Number of Cyber Attacks

Cyber incidents are the biggest worry for companies globally in 2024, according to the Allianz Risk Barometer. 2023 saw a worrying resurgence in activity, with insurance claims activity up by more than 50% compared with 2022.

In 2023, companies from Ireland (71%), Germany (58%), France (53%), US (51%), UK (49%) reported cyber attacks.

2

Type of Cyber Attacks

According to research commissioned by Sophos, 94% of 3,000 cybersecurity and IT leaders across 14 countries experienced some form of a cyberattack or security breach in 2022. The businesses were victims of phishing (27%), data exfiltration (26%), cyber extortion (24%) and ransomware (23%).

Cyber criminals are exploring ways to use new technologies such as generative artificial intelligence (AI) to automate and accelerate attacks.

3

Impact to Organizations

In 2022, 76% of organizations were targeted by a ransomware attack, out of which 64% were actually infected. Only 50% of these organizations managed to retrieve their data after paying the ransom.

Examples

Sources:

Biggest Data Breaches And Cyber Hacks of 2024 – Updated (techopedia.com)

Waren Sie betroffen? Die 5 heftigsten Hackerangriffe in Deutschland 2023 - CHIP

The biggest cyberattacks of 2023 - Tech Monitor

A cyber attack...

Our Learnings

1. 1) Set up Response Team
2. 2) Seek Expert Support
3. 3) Precautions to Take
4. 4) Inform and Engage

The Response Team

Key Members

Senior Executives from management, IT, HR, Banking, Sales/Marketing

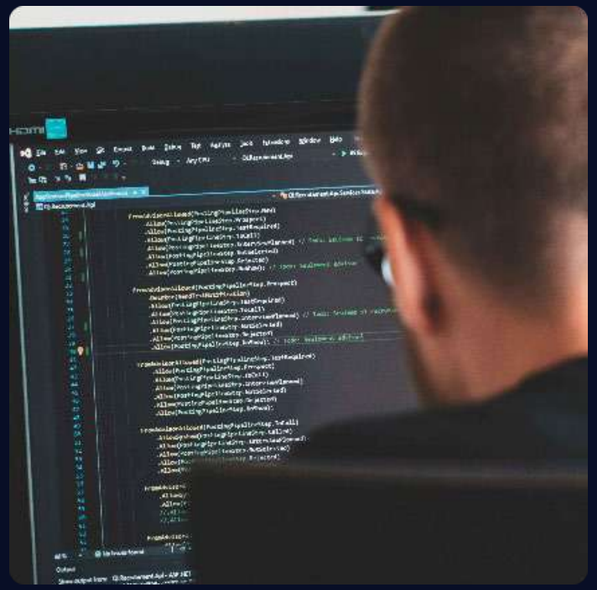
Daily Routine

Dividing responsibilities and reporting daily progress to ensure coordinated and efficient reaction to a cyber incident.

Responsibilities

Analysing situation and progress, making decisions to allocate resources, engaging with leaders and customers to preserve trust.

Expert Support



IT Experts

Detection, forensic analysis, threat intelligence, active defense, incident response and and recovery, infrastructure security…

Legal Experts

Review and approve communication for external and and internal use, guidance on legal reporting with authorities (GDPR…)

Cyber Security Consultants

Incident response, strategy and and negotiation with hackers

Precautions to Take

Financial Measures

Close bank accounts. Inform important stakeholders.

1

IT Measures

Shut down important (all) IT infrastructure. Secure backups. Buy new IT equipment and set up temporary network / email.

2

3

Employee Measures

Define emergency work plan. Inform employees and important stakeholders.

Inform and Engage

1 Employees

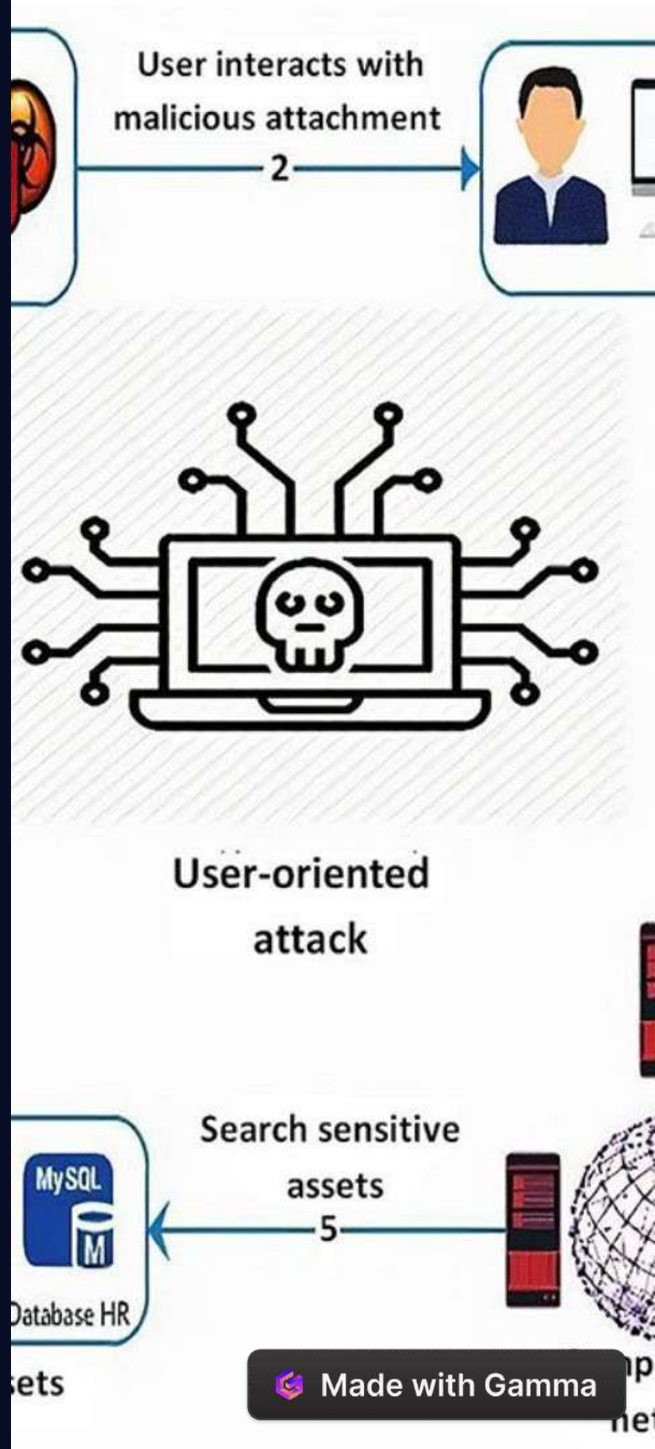
Set up communication channels. Provide regularly updates, clear guidelines and personal outreach.

2 Customers

Connect with customers to preserve trust. Provide guidelines to customer-facing staff.

3 Authorities and Third Parties

Ensure compliance with data protection regulations, mitigating legal and financial risks. Engage with vendors.



Best Practices for Managing Employees

- Communication Protocols
- Personal Outreach
- Emergency Work Plans
- Payroll Operations
- Data Security
- Ramp-Up Plan
- Training
- Care

Communication Protocols

Personal Outreach

Emergency Work Plans

Payroll Operations

Data Security

Ramp-Up Plan

Training

Care

Questions?