Trust Under Attack: Insider Threats in a Hyperconnected Enterprise

SS-Consulting
CYBER SECURITY SPECIALISTS

Introduction

Modern organisations are increasingly interconnected. Cloud platforms, third-party service providers, SaaS applications, AI productivity tools, and remote work have created highly efficient digital environments. However, these same technologies have also created new security risks.

One of the most concerning developments in today's threat landscape is the abuse of trust within organisations. Cyber-attacks increasingly begin not with traditional malware, but with compromised identities, manipulated employees, or trusted vendors whose access is exploited by adversaries.

In this challenge, your team will explore how insider threats and trust-based attacks can impact a large organisation operating in a highly digital environment.

An insider threat does not necessarily mean a malicious employee. It may include:

- employees manipulated through phishing or AI-generated impersonation
- compromised user identities
- abused access privileges
- third-party vendors whose credentials are exploited
- insiders who unintentionally expose sensitive systems

In such cases, attackers exploit the trust relationships inside organisations to move through systems and access sensitive information.

Tasks and Objectives

Your task is to examine how such an attack might unfold, and how organisations can defend themselves.

Your objective is to analyse a realistic insider-driven cyber-attack scenario and propose practical measures that organisations can take to prevent, detect, and respond to such threats.

You should approach this challenge from the perspective of a cybersecurity team advising organisational leadership.

Key questions to consider:

1. To guide your thinking, reflect on questions such as:
2. How could an attacker exploit trusted identities or insider access to gain entry into an organisation?
3. How might AI-enabled phishing, impersonation, or social engineering increase the risk of insider compromise?
4. Which systems or services within a modern organisation might be most vulnerable if insider access were abused?
5. What types of third-party vendors or service providers could create additional exposure?
6. What security practices could help organisations reduce the risk of insider-driven cyber-attacks?

These questions are intended to guide your analysis, you do not need to answer each one individually.

Key Tasks

Your 3-minute video proposal must cover the following:

Explain how an insider-style cyber-attack could impact a modern organization and how it could be prevented.

Think about a realistic situation where an attacker gains access by exploiting a trusted person, account, or external partner. For example, this could involve an employee being manipulated through AI-generated phishing or voice impersonation, stolen login credentials used to access cloud systems, a compromised vendor account, or an insider abusing excessive access privileges. Briefly describe how such an attack might occur and what the attacker could achieve.

You should also consider the organisation's digital environment and potential attack surface. Reflect on which systems or services might be most attractive targets for attackers, such as cloud platforms, employee accounts, connected applications and APIs, third-party vendors, or critical operational systems.

Finally, suggest practical steps organisations can take to reduce the risk of insider-driven attacks. These might include stronger identity and access controls, improved monitoring of suspicious behaviour, better vendor access management, enhanced authentication practices, and employee cybersecurity awareness training. Focus on the measures you believe would have the greatest impact in improving security.

Final Requirement

Your plan should be simple, practical, and realistic, helping the company protect its systems while ensuring that operations remain safe and uninterrupted.

April 7th, 12:00PM CET/SAST is the deadline for you to hand in a video of max. 3min to cyberschool@hcss.nl, in which you explain your Challenge solution and proposal. This is the final submission moment and from this submission, a Challenge-winning team will be determined. More information on this will be communicated via email.

Contributor

SS-Consulting is a cybersecurity and risk management consultancy focused on protecting sensitive information and critical systems. They work across cybersecurity, governance, risk, and compliance, with a practical and integrity-led approach to security.