Risk Assessment and Incident Response Plan for PowerPlus

An Information Security Analysis

Denis Ungureanu fc56307
Leonardo Monteiro fc58250
Gustavo Henriques fc64361

Prof. Dr. Ana Respício

Risk Analysis and Management in Information Security
MSc in Computer Science and Engineering

November 2024

Contents

Chapter 1

Introduction

1.1 Purpose of the Report

This report aims to conduct a comprehensive risk assessment and develop an initial incident response plan for PowerPlus. The project addresses the organization's need to protect its critical assets, secure its technological infrastructure, and manage cybersecurity risks. The findings will guide the Information Security and IT Risk Management teams in implementing effective controls and preparedness strategies for potential security incidents.

1.2 Background on PowerPlus

PowerPlus is a multinational energy company, focusing on managing critical infrastructure across Europe and the Americas. With 15,000 employees (including 5,000 external contractors), PowerPlus serves 20 million electricity and 1.3 million gas customers. Its strategic goals emphasize sustainability, innovation, expanding into new regions, boosting renewable energy, and advancing digital transformation. Operating within a highly regulated industry, PowerPlus complies with stringent sectoral and data privacy regulations, such as GDPR. The Information Security department, part of Corporate IT, works closely with a Corporate Risk division. Their infrastructure spans both Operational Technology (OT) and Information Technology (IT), necessitating tailored security protocols for each. A key component of PowerPlus's security is its Security Operations Center (SOC), which provides real-time monitoring, incident response, and vulnerability management. The IT environment includes 200 applications, cloud services, extensive data centers for disaster recovery, and a BYOD policy. These measures highlight PowerPlus's commitment to secure operations across a complex technological landscape.

1.2.1 Industry-Specific Security Challenges

Energy companies like PowerPlus face significant security challenges, including advanced persistent threats (APTs) from nation-state actors, ransomware attacks targeting critical systems, and vulnerabilities in their supply chains. Operational Technology (OT) security is especially crucial, as OT systems often lack the robust protections of IT networks. Insider

threats also pose risks, alongside the pressures of meeting regulatory compliance requirements, such as GDPR. These factors highlight the need for strong, layered cybersecurity measures to protect against frequent and evolving threats in the industry.

1.3 Objectives of the Risk Assessment and Incident Response Plan

This report outlines the key objectives of PowerPlus's risk assessment and incident response plan, developed to strengthen the organization's cybersecurity posture and ensure resilient business operations.

- **Cybersecurity Risk Identification and Evaluation:** The primary goal is to systematically identify, analyze, and assess cybersecurity risks affecting PowerPlus, focusing on critical infrastructure and identifying potential vulnerabilities within both IT and Operational Technology (OT) systems.
- **Proactive Incident Response Strategy:** PowerPlus aims to establish a proactive approach to cybersecurity incidents. By preparing strategies to respond effectively to potential threats, PowerPlus can minimize damage and facilitate quick recovery in the event of an incident.
- **Compliance with ISO/IEC 27005:2022 Standards:** The risk management framework is aligned with the ISO/IEC 27005:2022 standards, ensuring that PowerPlus follows systematic and industry-recognized practices in identifying and managing security risks.
- **Guidelines for the Security Operations Center (SOC):** Clear guidelines are set for the SOC to enable prompt detection, response, and mitigation of cybersecurity incidents. The SOC's protocols include real-time monitoring, analysis, and structured incident response to reduce the impact of threats.

1.4 Methodology Overview

This report will employ a structured methodology for risk assessment and incident response planning, grounded in industry-standard frameworks. The approach is as follows:

- **Primary Standard – ISO/IEC 27005:2022:** ISO/IEC 27005:2022 will serve as the main standard for guiding the risk assessment process, offering a comprehensive framework for systematically identifying, analyzing, evaluating, and treating cybersecurity risks specific to PowerPlus's infrastructure.
- **Supplementary Standards – ISO/IEC 27001:2022 and ISO 31000:2018:** To enhance the security and risk management framework, references will be made to ISO/IEC 27001:2022 for information security standards and ISO 31000:2018 for general risk management guidance, ensuring a holistic approach to risk and security.

- **Structured Risk Management Process:** The methodology will involve clearly defined phases of risk management: identifying potential risks, analyzing their likelihood and impact, evaluating them in the context of PowerPlus's operations, and developing appropriate treatments to mitigate or manage identified risks effectively.
- **Incident Scenarios and SOC Strategies:** Based on identified threats and vulnerabilities, specific incident scenarios will be developed. These scenarios will inform the preparation and response strategies for the Security Operations Center (SOC), ensuring that PowerPlus is equipped to handle various potential cybersecurity incidents with proactive and targeted responses.

1.5 Structure of the Report

- **Establishing the Context:** Defines the scope of the assessment, identifies PowerPlus's critical assets, outlines the risk environment, and describes the methodology used for evaluating cybersecurity risks.
- **Risk Assessment:** Documents the process and outcomes of identifying and evaluating risks that are specific to PowerPlus, providing insight into the organization's security landscape.
- **Incident Scenarios:** Presents three hypothetical attack scenarios to assess PowerPlus's readiness and resilience, helping to evaluate the effectiveness of current security measures.
- **SOC Preparation:** Details the monitoring requirements for PowerPlus's Security Operations Center (SOC) and provides three specific incident response cases, offering guidelines for effective response and mitigation.
- **Conclusions:** Summarizes the assessment's main findings and offers recommendations to enhance PowerPlus's cybersecurity posture.
- **References:** Lists all standards, frameworks, and resources cited in the report in APA format, ensuring proper attribution and traceability.

Chapter 2

Establishing the Context

2.1 Organizational considerations

2.1.1 Definition and Structure of the Organization

PowerPlus is defined as a group of entities working collaboratively to achieve its objectives within the energy sector. It includes internal and external teams:

- **Internal Workforce:** 10,000 employees working across corporate IT, operational technology (OT), and various business units.
- **External Workforce:** 5,000 external collaborators, supporting application maintenance, operations, and projects.

PowerPlus operates as a multifaceted organization encompassing IT and OT domains, with a central Corporate IT structure managing information security and risk management, and decentralized OT operations supported by individual subsidiaries.

2.1.2 Risk Appetite and Governance

PowerPlus's risk appetite is influenced by its:

- **Size and Complexity:** Operating in 12 countries, the organization serves 20 million electricity customers and 1.3 million gas customers, necessitating a robust risk framework.
- **Sectoral Dynamics:** Operating under stringent energy regulations in Europe and the Americas.
- **Strategic Goals:** Objectives such as digital transformation, renewable energy expansion, and maintaining controlled risks highlight a balanced approach to risk acceptance and mitigation.

2.1.3 Risk Ownership

PowerPlus ensures that risk ownership is clearly defined within its governance framework:

- **Accountability and Authority:** Risk owners, primarily at the corporate and business unit levels, are entrusted with the authority and responsibility to manage identified risks.
- **Specialized Departments:** The PP Risk Department and the Security Operations Center (SOC) play pivotal roles in overseeing and mitigating risks related to cybersecurity, operational disruptions, and compliance.

2.2 Identifying Basic Requirements of Interested Parties

A) Description of Information Security Controls Adopted by the Organization (PowerPlus) to Ensure Compliance with the ISO/IEC 27001:2022 Standard

PowerPlus adopts a series of information security controls aligned with the requirements of the ISO/IEC 27001:2022 standard, with a focus on protecting the confidentiality, integrity, and availability of information and organizational assets. The main controls are presented below, considering the organizational structure, technological reality, and challenges faced by PowerPlus.

Organizational Controls:

- **Information Security Policies (5.1):** PowerPlus has information security policies communicated and understood by all employees and stakeholders. The policies are aligned with corporate objectives and the ISO/IEC 27001:2022 standard.
- **Identity and Access Management (5.16, 5.18):** The company uses strict processes for access control, including the use of identity and access management tools. This involves managing the user lifecycle and assigning permissions in critical systems.
- **Supplier Management (5.19, 5.20):** PowerPlus ensures that information security is monitored across the entire supplier chain, with specific controls for data protection, especially with suppliers who maintain the applications used by the company.
- **Security Incident Management (5.24 to 5.27):** PowerPlus operates a 24/7 *Security Operations Center (SOC)* that monitors cybersecurity incidents in real-time, performing detection, response, and learning from previous incidents, using tools like *SIEM (Security Information and Event Management)*.

Human Controls:

- **Training and Awareness (6.3):** PowerPlus promotes continuous information security training for all employees, ensuring that everyone is up to date with policies and

procedures related to security. The *Information Security and IT Risk Management* department coordinates this training.

- **Disciplinary Process (6.4):** A formal disciplinary process is in place to handle security violations, ensuring that infractions are dealt with in an appropriate and transparent manner.
- **Post-Termination Responsibilities (6.5):** When an employee leaves the organization or changes roles, their security responsibilities are maintained and monitored to avoid risks to the organization.

Physical Controls:

- **Physical Security and Perimeters (7.1, 7.2):** PowerPlus adopts stringent physical security measures to protect sensitive areas from unauthorized access. Physical security is managed by one of the companies within the PowerPlus group and integrates appropriate perimeter control.
- **Protection Against Environmental Threats (7.5):** Critical infrastructure, including data centers and OT (Operational Technology) systems, is designed to withstand environmental threats such as natural disasters and ensure business continuity.

Technological Controls:

- **Protection Against Malware (8.7):** PowerPlus implements robust solutions to protect against malware, complemented by continuous awareness and education programs for employees.
- **Technical Vulnerability Management (8.8):** The *Security Operations Center* continuously assesses vulnerabilities and applies necessary corrections to mitigate risks. Penetration tests and forensic analysis are also periodically conducted.
- **Network and System Security (8.20, 8.21):** PowerPlus rigorously manages and monitors its networks and systems, ensuring that communication and data traffic are secure. *Oracle* and *SAP* technologies are widely used within the organization, with intensive access control and monitoring.

D) Specific international and/or national regulations

PowerPlus is subject to strict regulations due to its operations in the energy sector across different regions, including Europe and the American continent. These regulations aim to ensure the security, data privacy, and continuity of operations in a highly critical sector.

E) The organization's internal security rules

PowerPlus has established internal security rules that cover various aspects of information security, including the following:

- Ensures proper control of the user lifecycle and access rights to applications and systems.

- Monitors security incidents 24/7, conducts forensic analysis, manages vulnerabilities, and promotes security awareness among employees.

- Managed through a centralized SIEM (Security Information and Event Management) system, correlating data from more than 100 technological components.

F) Security rules and controls from contracts or agreements:

PowerPlus applies stringent security controls in contracts with suppliers, particularly regarding the maintenance of its applications and protection of personal data. These controls ensure continuity of IT services and compliance with security regulations.

G) Security controls implemented based on previous risk treatment activities:

The company implements security controls based on prior risk assessments, utilizing the Security Operations Center (SOC) and a SIEM system for monitoring and managing incidents and vulnerabilities. These controls also include identity and access management, ensuring continuous protection of data and systems.

2.3 Applying risk assesment

PowerPlus incorporates risk assessments across various organizational processes to ensure comprehensive risk management. These processes include:

- **Project Management:** Evaluating risks associated with implementing new projects, such as integrating renewable energy solutions or expanding into new geographies.

- **Vulnerability Management:** Regularly assessing technological vulnerabilities, especially within its operational technology (OT) and IT systems, which are managed under distinct domains.

- **Incident Management:** The Security Operations Center (SOC) operates 24/7 to detect, assess, and manage cybersecurity incidents, utilizing SIEM tools to analyze data from over 100 technological components.

- **Problem Management:** Addressing recurring issues, such as vulnerabilities in legacy SAP applications.

- **Impromptu Risk Assessments:** Tackling specific ad-hoc concerns, such as risks associated with BYOD policies or cloud services managing personal data.

2.4 Establishing and maintaining information security risk criteria

2.4.1 General

PowerPlus establishes and maintains information security risk criteria based on the requirements of ISO/IEC 27001:2022 ((section 6.1.2.a)) and ISO/IEC 27005:2022. These criteria are designed to ensure that:

- Risks are assessed consistently, ensuring reliable and comparable results.
- Decisions on risk treatment and acceptance are aligned with strategic objectives and organizational capacity.

The criteria used are as follows:

- Impact on organizational objectives Here the potential costs of an outage (e.g., lost revenue, regulatory fines) are evaluated in financial terms. The reputational impact if the incident happens is also assessed. In addition, the impact that the risk will have on the continuity of the company's services is analysed and whether we are going against specific rules of the energy sector in this case.
- Likelihood A historical analysis is made to understand the probability that the risk will have to happen.
- CIA The potential leakage of sensitive information (confidentiality) is analyzed. In addition to data leakage, it is necessary to understand if the data remains accurate and reliable, so as not to affect integrity. Finally, it is also important to understand the company's availability when suffering a certain attack.
- Response time and recovery Another important criteria is the time that the sistem that to recover from an incident.
- Combination e Risk Sequence Analyze how multiple risks can occur simultaneously.

2.4.2 Risk acceptance criteria

Risk acceptance criteria sets out the guidelines that PowerPlus uses to determine whether an identified risk is acceptable or requires further treatment. These criteria are key to ensuring consistency in the risk management process, aligning risk acceptance decisions with risk appetite, strategic objectives, and organizational constraints. In this section, acceptable risk levels, authorities responsible for taking such decisions, conditions for risk acceptance and review and adjustment of criteria will be defined.

Risk Levels

Low risks have a low probability of occurrence and reduced impact. Generally, these risks do not affect critical systems such as OT and IT, nor regulatory compliance. Because they are

considered of little relevance, they can be accepted without the need for additional measures. Medium risks have a moderate probability or impact. While not critical, they can cause significant disruptions to important processes such as internal IT operations or customer service. These risks are analyzed more closely and generally accepted based on existing controls, but they are regularly monitored to prevent them from evolving to more critical levels. High risks, on the other hand, have a high probability of occurrence and/or serious impact. These risks can compromise the continuity of critical services, lead to regulatory breaches, or cause the loss of sensitive customer data. Due to their severity, these risks are not directly accepted and require immediate treatment, such as the implementation of additional controls or specific mitigation measures.

Risk Acceptance Authority

At PowerPlus, risk acceptance is distributed according to severity and hierarchical level. Low risks are accepted by operational managers, while medium risks require approval from directors, especially if they affect strategic systems. High risks, which can compromise critical systems or violate regulations, are analyzed by senior management or the risk committee. This structure ensures decisions aligned with the organization's strategic objectives and risk appetite.

Conditional acceptance

For example, a risk associated with a legacy system may be temporarily accepted while a technology refresh plan is being executed. Similarly, conditional acceptance can be applied in scenarios where a high risk is unavoidable, but mitigation strategies such as contingency plans or enhanced monitoring are in place to minimize potential impacts. These conditions ensure flexibility in risk management, without compromising PowerPlus' security or regulatory compliance.

Review and Adjustment of Criteria

PowerPlus' risk acceptance criteria will be reviewed annually to ensure that they remain aligned with changes in the organizational context, such as technological upgrades, regulatory changes, or changes in strategic objectives. This includes an ongoing analysis of factors such as new cyber threats, modifications to business processes, and the evolution of IT and OT infrastructure.

The review of the criteria also considers feedback from security incidents or resilience tests carried out by the organization, adjusting the acceptance criteria as necessary. With this, PowerPlus ensures that its risk acceptance criteria remain effective, ensuring the continuous protection of critical assets and compliance with legal obligations.

2.4.3 Criteria for performing information security risk assessments

General

Criteria for performing information security risk assessments is essential to define clear and consistent criteria for the assessment of information security risks, ensuring that risks are analyzed effectively. These criteria aim to determine the significance of risks in terms of their consequences, probability of occurrence and level of risk. The definition of such criteria must consider factors such as the classification of information, the quantity and concentration of data, the strategic importance of the business processes involved, as well as the operational criticism of the availability, confidentiality, and integrity of information.

Consequence Criteria

Here are the consequence criteria for PowerPlus, taking into account the company's context in the renewable energy sector and its technological operations:

- **Minor:** Negligible consequences for PowerPlus.
  No significant operational impact on energy generation activities and no risks to the safety of people or property.
  Example: A minor failure in a secondary system that consumes operational margins but does not affect the organization's objectives.

- **Significant:** Limited but relevant consequences for PowerPlus.
  Partial degradation of activities, such as temporary reductions in energy generation efficiency, without endangering the safety of people or assets.
  Example: A failure in a single wind turbine causing reduced output but allowing continued operation in a degraded mode.

- **Serious:** Substantial consequences for PowerPlus.
  Significant operational degradation with potential implications for the safety of people or assets.
  Example: Simultaneous failures in several energy assets resulting in a disruption of a significant portion of energy supply, creating severe operational challenges but no direct impact on the energy sector as a whole.

- **Critical:** Disastrous consequences for PowerPlus.
  Inability to maintain essential activities, with serious consequences for the safety of people or property.
  Example: A catastrophic failure in a solar plant leading to fires or significant damage, threatening the company's continuity and possibly impacting sectors reliant on the energy provided.

- **Catastrophic:** Consequences beyond PowerPlus, affecting the energy sector or society at large.
  Substantial impact on the renewable energy sector, with potential regulatory or environmental implications.

Example: A major incident involving the company's infrastructure, causing severe environmental pollution or widespread energy outages, affecting critical sectors and requiring governmental response.

Likelihood Criteria

In this section on Likelihood criteria, the objective is to define how the probability of a risk occurring will be assessed. That is, we need to specify how the company will determine the chance of a risk occurring based on different factors. To do that it is necessary to specify the factors that can influence the probability and to show how a probability is going to be measure, using a scale.

Factors that can influence the probability

- Accidental or natural events Natural disasters or industrial accidents can increase the likelihood of service disruptions.
- Exposure of information or assets Exposure of critical data or systems to the internet or threats increases risk.
- Exploitable vulnerabilities Security flaws or outdated systems make risks more likely.
- Technology failures Hardware or software problems, common in power systems, increase the risk of operational failures.
- Human errors Failures due to negligence or lack of training can increase the likelihood of incidents.

Probability measurement

To measure the likelihood of risks at PowerPlus, the following qualitative scale will be used:

- **0 - Not Applicable:** 0% likelihood in the next 12 months. *(Will never happen).*
- **1 - Rare:** 5% likelihood in the next 12 months. *(May happen once every 20 years).*
- **2 - Unlikely:** 25% likelihood in the next 12 months. *(May happen once every 10 years).*
- **3 - Moderate:** 50% likelihood in the next 12 months. *(May happen once every 5 years).*
- **4 - Likely:** 75% likelihood in the next 12 months. *(May happen once every year).*
- **5 - Almost Certain:** 100% likelihood in the next 12 months. *(May happen multiple times a year).*

To determine the chance of a risk occurring, we can look at how often similar events have occurred in the past. If, for example, technological failures or operational failures have already occurred several times, the chance of occurrence increases.

Criteria for determining the level of risk

The level of risk is determined by analyzing the combination of the likelihood of an event occurring and the severity of its consequences. The following matrix will guide the risk evaluation process:

Likelihood	Catastrophic	Critical	Serious	Significant	Minor
Almost certain	Very high	Very high	High	High	Medium
Likely	Very high	High	High	Medium	Low
Moderate	High	High	Medium	Low	Low
Unlikely	Medium	Medium	Low	Low	Very low
Rare	Low	Low	Low	Very low	Very low
Not applicable	Very low	Very low	Very low	Very low	Very low

Table 2.1: Risk Level Matrix for PowerPlus

Explanation of the Risk Matrix:

- **Likelihood Levels:** The likelihood of an event is categorized into six levels: Almost certain, Likely, Moderate, Unlikely, Rare, and Not applicable, as defined earlier.
- **Consequence Levels:** Consequences are categorized from Catastrophic to Minor, as defined in the consequence criteria.
- **Risk Ratings:** The intersection of likelihood and consequence determines the risk rating (e.g., Very High, High, Medium, Low, Very Low).
- **Purpose:** This matrix helps prioritize risks, ensuring that resources are allocated to mitigate the most critical risks effectively.

2.5 Choosing an Appropriate Method for Information Security Risk Assessment at PowerPlus

In the context of PowerPlus, the selection of a method for managing information security risks must align with the organization's overall risk management approach, as defined in **ISO/IEC 27001:2022, 6.1.2 b)**. This method must ensure that risk assessments are **consistent**, **valid**, and **comparable**.

2.5.1 Consistency

To ensure consistency, risk assessments should follow a standardized process where the same risks, when evaluated by different individuals or at different times, yield similar results. At PowerPlus, this can be achieved through tools like **SIEM (Security Information and Event Management)**, which correlates data from various sources for continuous and consistent monitoring of security incidents.

2.5.2 Comparability

PowerPlus should define clear and uniform risk assessment criteria to enable objective comparisons between different risks. A **risk matrix** based on impact and likelihood can be used to classify risks in both IT (Information Technology) and OT (Operational Technology), ensuring that decisions are aligned with business strategy.

2.5.3 Validity

The validity of risk assessments depends on their adherence to operational reality. This requires using **real-world scenarios** and **updated data** on vulnerabilities and impacts. PowerPlus should consider:

- **200 corporate applications** handling critical data;
- **6 million personal data records**;
- **Cloud services (SaaS and IaaS)**, which expand the attack surface.

Periodic assessments and audits will help continuously validate the results, ensuring compliance with changes in the threat landscape.

We conclude that adopting a risk management method that ensures **consistency**, **comparability**, and **validity** will enable PowerPlus to meet the requirements of **ISO/IEC 27001:2022** and strengthen its information security, supporting its objectives of growth, innovation, and risk control.

Chapter 3

Risk Assessment

3.1 Risk identification

Risk identification is a critical component of the overall risk assessment process. The following eight risks are identified as the most significant for PowerPlus, based on its organizational and technological context, in alignment with ISO/IEC 27005:2022:

1. **Data Breaches Affecting Personal Data**
    - *Description:* With 20 applications handling 6 million customer records and the use of cloud services (SaaS and IaaS), there is a high risk of data breaches compromising customer data confidentiality.
    - *Proposed Control:* Implement robust encryption, multi-factor authentication (MFA), and regular audits of data access policies.
    - *Risk Owner:* Data Protection Officer (DPO) or Information Security Manager.
    - *Reason:* Responsible for overseeing compliance with data protection regulations and managing risks related to customer data confidentiality.
2. **Unsecured Remote Maintenance for OT Systems**
    - *Description:* Operational Technology (OT) systems rely on remote maintenance through vendor-contracted services, exposing them to potential vulnerabilities in external access points.
    - *Proposed Control:* Enforce strict VPN configurations, role-based access control, and monitor remote maintenance activities with real-time logging.
    - *Risk Owner:* Head of Operational Technology (OT) Security
    - *Reason:* Accountable for the security of OT systems and ensuring that remote access by external vendors is managed securely.
3. **Inadequate Management of Legacy Systems**
    - *Description:* PowerPlus uses legacy SAP technologies over 15 years old, which are prone to vulnerabilities due to outdated components.

- *Proposed Control:* Implement a phased modernization plan for legacy systems and deploy virtual patching solutions to mitigate risks in the interim.
- *Risk Owner:* IT Infrastructure Manager
- *Reason:* Oversees the maintenance and modernization of legacy systems and ensures continuity and security during transitions.

4. **BYOD Policy Risks**

   - *Description:* The Bring Your Own Device (BYOD) policy, without restrictions on platforms or devices, poses risks of unauthorized access and data leaks.
   - *Proposed Control:* Deploy Mobile Device Management (MDM) tools and enforce endpoint security measures.
   - *Risk Owner:* IT Policy and Compliance Manager
   - *Reason:* Accountable for enforcing IT policies, including BYOD standards, and ensuring endpoint security compliance.

5. **Physical and Logical Separation Challenges in Data Centers**

   - *Description:* The data centers, despite being distanced 100 km apart, may face risks related to improper disaster recovery configurations or simultaneous environmental hazards.
   - *Proposed Control:* Regularly test disaster recovery plans, enhance redundancy systems, and improve environmental monitoring.
   - *Risk Owner:* Data Center Operations Manager
   - *Reason:* Responsible for ensuring physical and logical security, disaster recovery planning, and minimizing environmental hazards.

6. **Insider Threats in Call Center Operations**

   - *Description:* Call centers with 300 agents require access to internal systems, increasing the risk of insider threats, including unauthorized data access or misuse.
   - *Proposed Control:* Implement strict identity and access management (IAM) systems and conduct periodic employee training on security protocols.
   - *Risk Owner:* Call Center Operations Manager
   - *Reason:* Accountable for managing access to internal systems by call center employees and mitigating potential insider threats.

7. **Complexity in Identity and Access Management (IAM)**

   - *Description:* Managing user lifecycles and access for 200 applications poses risks of misconfigurations and unauthorized access.
   - *Proposed Control:* Centralize IAM with automated provisioning and de-provisioning, coupled with periodic access reviews.
   - *Risk Owner:* Identity and Access Management Lead

- *Reason:* Directly responsible for implementing and maintaining centralized IAM systems and overseeing periodic access reviews.

8. **Insufficient Threat Detection Capabilities**

   - *Description:* Despite a 24/7 Security Operations Center (SOC) and SIEM tools, correlating events across 100 components might lead to undetected threats due to insufficient resources or system limitations.
   - *Proposed Control:* Enhance threat detection capabilities by integrating AI-driven analytics and increasing SOC workforce capacity.
   - *Risk Owner:* Security Operations Center (SOC) Manager
   - *Reason:* Manages the SOC team and ensures threat detection and response capabilities are effective and aligned with organizational needs.

3.2 Risk Analysis

The following is a hybrid analysis of the identified risks, evaluating their consequences and likelihood using a combination of qualitative and quantitative criteria:

1. **Data Breaches Affecting Personal Data**

   - **Consequence:** 4 - Critical (Quantitative estimate: Potential fines of up to €10M or 2% of global revenue under GDPR, significant reputational damage, and loss of customer trust).
   - **Likelihood:** 3 - Moderate (50% likely in the next 12 months. May happen once every 5 years).
   - **Level of Risk:** High (Combination of critical consequences and moderate likelihood).

2. **Unsecured Remote Maintenance for OT Systems**

   - **Consequence:** 5 - Catastrophic (Quantitative estimate: Operational disruptions costing €500K per day, plus regulatory penalties for outages in critical infrastructure).
   - **Likelihood:** 4 - Likely (75% likely in the next 12 months. May happen once every year).
   - **Level of Risk:** Very High (Combination of catastrophic consequences and likely likelihood).

3. **Inadequate Management of Legacy Systems**

   - **Consequence:** 3 - Serious (Quantitative estimate: Costs to address outages and patch vulnerabilities could reach €200K annually, along with potential productivity losses).

- **Likelihood:** 4 - Likely (75% likely in the next 12 months. May happen once every year).
- **Level of Risk:** High (Combination of serious consequences and likely likelihood).

4. **BYOD Policy Risks**

   - **Consequence:** 2 - Significant (Quantitative estimate: Data leaks or breaches from unsecured devices could cost up to €150K, affecting customer data or intellectual property).
   - **Likelihood:** 3 - Moderate (50% likely in the next 12 months. May happen once every 5 years).
   - **Level of Risk:** Medium (Combination of significant consequences and moderate likelihood).

5. **Physical and Logical Separation Challenges in Data Centers**

   - **Consequence:** 4 - Critical (Quantitative estimate: A dual data center failure could result in recovery costs exceeding €1M and disrupt services for millions of customers).
   - **Likelihood:** 2 - Unlikely (25% likely in the next 12 months. May happen once every 10 years).
   - **Level of Risk:** Medium (Combination of critical consequences and unlikely likelihood).

6. **Insider Threats in Call Center Operations**

   - **Consequence:** 3 - Serious (Quantitative estimate: Misuse of sensitive customer data could lead to fines and reputational harm amounting to €200K annually).
   - **Likelihood:** 3 - Moderate (50% likely in the next 12 months. May happen once every 5 years).
   - **Level of Risk:** Medium (Combination of serious consequences and moderate likelihood).

7. **Complexity in Identity and Access Management (IAM)**

   - **Consequence:** 3 - Serious (Quantitative estimate: Misconfigurations could lead to unauthorized access incidents costing €300K annually).
   - **Likelihood:** 4 - Likely (75% likely in the next 12 months. May happen once every year).
   - **Level of Risk:** High (Combination of serious consequences and likely likelihood).

8. **Insufficient Threat Detection Capabilities**

   - **Consequence:** 5 - Catastrophic (Quantitative estimate: A significant undetected cyberattack could lead to losses exceeding €1M, including downtime, recovery costs, and fines).

- **Likelihood:** 4 - Likely (75% likely in the next 12 months. May happen once every year).
- **Level of Risk:** Very High (Combination of catastrophic consequences and likely likelihood).

3.3 Risk Evaluation

Comparing the Results of Risk Analysis with the Risk Criteria

The purpose of this section is to compare the results of the risk analysis with Power-Plus's defined risk acceptance criteria. This ensures that identified risks are aligned with the organization's risk appetite, strategic objectives, and operational constraints.

- Risk acceptance criteria, as defined in Section 2.4.2, including thresholds for low, medium, and high risks.
- Risks with assigned level values based on the combination of consequences and likelihood.

The results of this comparison are summarized as follows:

- **Data Breaches Affecting Personal Data:** Categorized as a **Very High Risk**. Requires immediate treatment to prevent regulatory breaches and reputational harm. Suggested actions include strengthening encryption, performing regular audits, and enhancing access controls.
- **Unsecured Remote Maintenance for OT Systems:** Categorized as a **High Risk**. Immediate treatment is critical to secure remote access and prevent exploitation. Recommended actions include strict VPN configurations, role-based access, and real-time monitoring.
- **Inadequate Management of Legacy Systems:** Categorized as a **High Risk**. Conditional acceptance is possible while implementing a technology refresh plan. Virtual patching and strict monitoring are essential during the transition.
- **BYOD Policy Risks:** Categorized as a **Medium Risk**. Accepted based on existing MDM controls and endpoint monitoring but requires periodic review to ensure no escalation.
- **Physical and Logical Separation Challenges in Data Centers:** Categorized as a **Medium Risk**. Accepted based on the adequacy of current disaster recovery measures and geographical separation.
- **Insider Threats in Call Center Operations:** Categorized as a **Medium Risk**. Accepted with ongoing monitoring and regular employee training to mitigate insider threats.

- **Complexity in Identity and Access Management (IAM):** Categorized as a **High Risk**. Requires treatment to reduce misconfiguration and unauthorized access incidents. Centralized IAM implementation is a priority.
- **Insufficient Threat Detection Capabilities:** Categorized as a **Very High Risk**. Immediate treatment is critical to improve SOC operations and implement advanced threat detection tools.

3.3.1 Prioritizing the Analyzed Risks for Risk Treatment

The risks are prioritized for treatment based on the assessed levels, organizational objectives, and the views of relevant stakeholders.

The prioritization of risks for treatment is determined as follows:

- **High Risks:** Immediate priority for treatment. These risks are escalated to senior management or the risk committee for decision-making and action planning.
- **Medium Risks:** Treated based on a case-by-case analysis of existing controls. Monitoring and periodic reviews are critical to prevent escalation.
- **Low Risks:** Accepted without additional measures but monitored for any changes in conditions or context.

A prioritized list of risks is provided below:

1. **Unsecured Remote Maintenance for OT Systems**: Very High
2. **Insufficient Threat Detection Capabilities**: Very High
3. **Data Breaches Affecting Personal Data**: High
4. **Inadequate Management of Legacy Systems**: High
5. **Complexity in Identity and Access Management (IAM)**: High
6. **BYOD Policy Risks**: Medium
7. **Insider Threats in Call Center Operations**: Medium
8. **Physical and Logical Separation Challenges in Data Centers**: Medium

Chapter 4

Incident Scenarios

This chapter conceptualizes three potential attack scenarios that the PowerPlus SOC might face, highlighting the tactics, techniques, and procedures (TTPs) adversaries may employ. For each scenario, the attack phases and potential impact are described.

4.1 Scenario 1: Supply Chain Attack on Software Update Process

Description:
A threat actor compromises the software update process of a third-party vendor used by PowerPlus, embedding malicious code into a critical system update. The malicious update is installed on PowerPlus servers, creating a backdoor that allows attackers to exfiltrate sensitive data and move laterally across the IT and OT environments.

Attack Phases:

1. Initial Compromise: Exploitation of vulnerabilities in the vendor's development environment.

2. Propagation: Malicious updates are distributed to PowerPlus.

3. Execution: Backdoor activation, data exfiltration, and lateral movement within the network.

Potential Impact:

- Unauthorized access to sensitive customer and operational data.

- Risk of manipulation of OT systems, disrupting energy distribution.

- Reputational damage due to breach disclosure.

4.2 Scenario 2: Insider Threat Exploiting Privileged Access

Description:
A disgruntled employee with privileged access to PowerPlus's IT infrastructure sabotages critical systems by deleting customer databases and encrypting backups. The insider also disables monitoring tools to delay detection.

Attack Phases:

1. Preparation: Employee plans the attack by identifying high-value assets and disabling security measures.
2. Execution: Deletion of databases and encryption of backup systems.
3. Obfuscation: Disabling of monitoring tools to delay response.

Potential Impact:

- Loss of critical customer data, affecting 6 million clients.
- Disruption of business operations, including billing and CRM systems.
- Significant financial and reputational losses.

4.3 Scenario 3: Distributed Denial of Service (DDoS) Attack Targeting OT Systems

Description:
A group of hacktivists launches a large-scale DDoS attack against PowerPlus's OT infrastructure, targeting energy distribution management systems. The attack aims to overwhelm systems with traffic, causing operational disruptions and potential blackouts.

Attack Phases:

1. Reconnaissance: Hacktivists identify IP addresses and vulnerabilities in exposed OT systems.
2. Attack Launch: Botnets flood OT systems with traffic to overwhelm resources.
3. Sustainment: Attackers maintain high traffic volumes to prolong downtime.

Potential Impact:

- Disruption of energy distribution to residential and industrial customers.
- Financial losses due to service interruptions and SLA penalties.
- Decreased trust from regulators and customers.

Chapter 5

SOC Preparation

Security Operations Center (SOC) Functions – PowerPlus

1. Aspects to be Monitored by the SOC

Log Collection

Description:
PowerPlus must implement centralized log collection from all critical systems, including servers, databases, IT/OT applications, network devices, and BYOD endpoints.

Objective:
Enable real-time monitoring of security events, providing a comprehensive view of activities across the infrastructure.

Recommendations:

- Integrate 200 applications and OT devices with the SIEM solution for log collection.
- Capture critical logs related to remote access by external vendors responsible for OT system maintenance.

Aggregation/Correlation

Description:
PowerPlus must correlate security events from different sources to identify patterns that may indicate threats.

Objective:
Detect complex attacks that might go unnoticed in isolated analyses.

Recommendations:

- Configure correlation rules to monitor unauthorized access between IT and OT systems, preventing lateral movement between critical environments.

- Monitor the 20 applications handling personal data of 6 million customers for suspicious activities.

SIEM (Security Information and Event Management)

Description:
PowerPlus already utilizes a SIEM platform for security event integration and correlation. The SIEM will be the core of the SOC, aggregating, analyzing, and alerting on potential incidents.

Objective:
Provide a centralized view of security operations and detect threats in real-time.

Recommendations:

- Ensure that the SIEM is configured to integrate logs from 1,500 production servers, as well as critical cloud applications (SaaS and IaaS).
- Regularly review and update correlation rules in the SIEM based on new attack scenarios.

Threat Intelligence

Description:
PowerPlus should integrate threat intelligence feeds into the SOC to anticipate new attacks and vulnerabilities.

Objective:
Enhance the SOC's proactive capability to prevent incidents before they occur.

Recommendations:

- Subscribe to global and industry-specific threat intelligence feeds, especially for the energy sector.
- Monitor vulnerabilities specific to Oracle and SAP technologies, widely used in PowerPlus systems.

Research & Development (R&D)

Description:
The SOC should invest in developing new tools, techniques, and strategies to address emerging threats.

Objective:
Keep the SOC updated and prepared to face new security challenges.

Recommendations:

- Develop automated scripts for security monitoring in hybrid environments (on-premises and cloud).
- Conduct regular penetration tests on legacy SAP systems to identify and mitigate vulnerabilities.

Ticketing

Description:
The SOC must use an incident management system to track, prioritize, and resolve security incidents.

Objective:
Ensure that each incident is appropriately handled and resolved within defined timelines.

Recommendations:

- Implement a ticketing system integrated with the SIEM, with workflows prioritizing critical incidents in systems handling personal data and OT operations.
- Log all incidents involving remote access by vendors.

Knowledge Base

Description:
The SOC should maintain a repository of information on past incidents, response procedures, and best practices.

Objective:
Accelerate response to future incidents by reusing previously tested solutions.

Recommendations:

- Document critical incidents involving OT and IT systems, detailing mitigation measures.
- Create a repository of response procedures for ransomware attacks, given the criticality of energy systems.

Reporting

Description:
The SOC should generate periodic reports on the organization's security posture and the performance of security operations.

Objective:
Provide insights to senior management on PowerPlus's security posture and areas for improvement.

Recommendations:

- Develop monthly reports detailing critical incidents, unauthorized access attempts, and detected vulnerabilities.
- Present key performance indicators (KPIs), such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

2. Incident Response Cases

This section presents three detailed incident scenarios focusing on the response actions taken by the SOC.

5.0.1 Incident Response Case 1: Ransomware Attack on IT Infrastructure

Description: A ransomware attack encrypts critical IT systems, including production servers and databases that store customers' personal data.

Impact:

- Unavailability of billing and CRM systems.
- Potential leakage of personal data from 6 million customers.

Response Procedure:

1. Initial detection by the SIEM, which identified anomalous activities on the production servers.
2. Immediate isolation of the affected systems to prevent the ransomware from spreading.
3. Execution of backups to restore critical systems.
4. Communication with cloud providers to ensure the security of cloud environments.

Lessons Learned:

- Implement stricter network segmentation.
- Regularly update backup policies.

5.0.2 Incident Response Case 2: Phishing Attack Targeting Employees

Description: A phishing campaign targets Call Center employees to steal credentials for accessing internal systems.

Impact:

- Unauthorized access to customers' personal data.
- Potential compromise of administrative accounts.

Response Procedure:

1. SIEM detects suspicious logins from unknown IP addresses.
2. Immediate blocking of compromised accounts and password resets.
3. Notification and training of employees about the phishing campaign.
4. Review of SIEM correlation rules to detect similar patterns in the future.

Lessons Learned:

- Implement Multi-Factor Authentication (MFA) for all critical systems.
- Increase the frequency of security awareness training.

5.0.3 Incident Response Case 3: Remote Access Breach on OT Systems

Description: Unauthorized remote access to OT systems through compromised credentials of third-party vendors.

Impact:

- Risk of compromise to energy control systems.
- Potential disruption in the energy supply to customers.

Response Procedure:

1. SIEM detects repeated login attempts outside vendors' working hours.
2. Blocking of remote access and notification to OT system managers.
3. Audit of access logs to identify potential compromises.
4. Implementation of secure remote access solutions (VPNs and zero trust policies).

Lessons Learned:

- Improve network segmentation between IT and OT environments.
- Establish stricter remote access policies for third-party vendors.

Conclusion

Establishing an efficient Security Operations Center (SOC) is crucial for PowerPlus to address cybersecurity risks. Centralized log collection, event correlation, threat intelligence, and continuous innovation are key to detecting and mitigating security incidents. The incident response cases highlight the importance of swift actions and adopting best practices such as network segmentation and employee training. With a robust SOC, PowerPlus will be better equipped to protect its infrastructure and data, ensuring the continuity of critical operations.

Chapter 6

Conclusions

This report provides a comprehensive evaluation of the cybersecurity posture of PowerPlus, highlighting the critical importance of robust risk assessment and incident response planning. PowerPlus operates within a highly regulated energy sector, facing unique challenges that demand tailored and proactive cybersecurity measures.

The findings emphasize the need for a structured and consistent approach to risk management, aligning with industry standards like ISO/IEC 27005:2022. Key achievements include the identification and analysis of risks such as data breaches, unsecured remote access, and the complexities of managing legacy systems. The use of advanced methodologies and frameworks ensures that these risks are prioritized and addressed effectively.

Additionally, incident scenarios and Security Operations Center (SOC) preparation are pivotal in demonstrating PowerPlus's readiness to mitigate threats. The SOC's critical functions, including log collection, event correlation, and the integration of threat intelligence, are foundational to its capability to detect and respond to security incidents efficiently. Incident response case studies further illustrate the organization's capacity to handle real-world threats, emphasizing swift and informed decision-making to mitigate impact.

The recommendations presented in this report provide actionable insights for enhancing the organization's cybersecurity infrastructure. These include the adoption of AI-driven analytics, the reinforcement of access controls, and the continuous training of personnel. Furthermore, a commitment to periodic reviews of risk acceptance criteria and vulnerability assessments will ensure that PowerPlus remains agile and resilient in the face of evolving cyber threats.

In conclusion, this report underscores the imperative for PowerPlus to maintain a robust cybersecurity framework. By prioritizing risk mitigation, leveraging innovative technologies, and fostering a culture of security awareness, PowerPlus can safeguard its operations, protect its critical assets, and uphold its commitment to regulatory compliance and customer trust.

Chapter 7

References

1. APA Style (2016). Quick Answers — References. Accessed November 2, 2023. http://www.apastyle.org/learn/quick-guide-on-references.aspx

2. ISO (2018). NP ISO 31000:2018 – Gestão do risco – Linhas de orientação. International Organization for Standardization. https://www.iso.org/standard/65694.html

3. ISO/IEC (2022a). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems. International Organization for Standardization and International Electrotechnical Commission.

4. ISO/IEC (2022b). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization and International Electrotechnical Commission.

5. Ross, R. S., et al. (2012). Guide for Conducting Risk Assessments (NIST SP-800-30rev1). The National Institute of Standards and Technology (NIST), Gaithersburg. Accessed November 2, 2023. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

6. CIS (2024). Center for Internet Security Critical Security Controls v8. https://www.cisecurity.org/controls/cis-controls-list