Cybersecurity Efforts undertaken at BESSY II

Journal of Physics: Conference Series **3010** (2025) 012022 doi:10.1088/1742-6596/3010/1/012022

Cybersecurity Efforts undertaken at BESSY II

R. Müller, M. Meier, B. Grabowski, D. Herrendörfer, R. Ovsyannikov, A. Schälicke, J. Viefhaus, and A. Jankowiak

Helmholtz-Zentrum Berlin (HZB), Albert-Einstein-Strasse 15, 12489 Berlin, Germany

E-mail: roland.mueller@helmholtz-berlin.de

Abstract.

Synchrotron facilities are adopting open science principles, emphasizing online access and remote experimentation while addressing cybersecurity challenges. Helmholtz-Zentrum Berlin (HZB) has strengthened the security protocols for its light source BESSY II, using a defense-in-depth approach, which is standard in accelerator environments. This paper outlines these measures and broader efforts of HZB to balance threat mitigation with user needs, leveraging documented attack methods and governance frameworks to enhance cybersecurity in the synchrotron field.

1 Introduction

The widespread adoption of remote access at synchrotron facilities, accelerated by the changed user needs during the COVID-19 pandemic, has enabled users to conduct experiments remotely and increases automation capabilities. This operational shift demands robust digital infrastructure supporting hybrid experimentation models. Concurrently, the cybersecurity landscape has evolved from individual threats to sophisticated criminal enterprises, monetizing system vulnerabilities and ransomware services.

As publicly funded institutions are prohibited from paying ransoms, research facilities must prioritize preventive cybersecurity and recovery protocols. This requirement presents unique challenges for BESSY II's open science infrastructure, where HZB manages complex legacy systems. The facility's operational priorities of rapid experimental commissioning and continuous user access have resulted in a flat network architecture with decentralized oversight, complicating security modernization efforts.

Accessibility was prioritized at BESSY II during the rapid transition from pilot beamline commissioning to serving over 50 instruments in time-sharing mode on a compact ring with only 16 segments, but this heightened cybersecurity risks. A brief cyberattack in June 2023 caused significant system damage despite minimal data loss. Although clean systems were restored from backups, the compromised infrastructure necessitated a complete reconstruction of the synchrotron's user data acquisition environment.

2 Vulnerability Analysis

The central IT infrastructure at HZB is built on Microsoft Windows platforms, with Active Directory/Domain Controller (AD/DC) managing system assets, user identities, and software lifecycles across general-purpose networks. While AD/DC offers robust capabilities and convenience for IT maintenance, it also presents a critical vulnerability, as its compromise by attackers could result in extensive damage. At HZB, only the light source accelerators and proton medical therapy systems operate within isolated technical networks, independent of this infrastructure.

Accelerator
Accelerators supporting all experiments must prioritize maximum availability and minimal downtime, necessitating a reliable control system and robust IT infrastructure to ensure optimal process performance. Connectivity and real-time responsiveness are fundamental requirements. A classified technical network that is autonomous, self-contained, and isolated from the broader IT environment is crucial for IT security [1]. Such a network must permit only limited, audited access and be protected by firewalls to prevent unauthorized activities and cross-domain interference, even from internal systems such as office networks. Vulnerable devices require secure environments, and cybersecurity measures against external threats are just one component of comprehensive accelerator protection strategies. Consequently, the dedicated HZB accelerator network and domain-specific IT remained largely unaffected by the cyberattack.

Instruments and Data Acquisition
The initial generation of beamlines and instruments was implemented in a coordinated manner, allowing effective management of failure scenarios, surveillance, and control of attack surfaces. However, subsequent instrument additions and extensions were developed through project-based approaches characterized by rapid prototyping and customized workflows. These additions were often carried out under tight time constraints, employing IT components and tools tailored to meet short-term milestones. Security measures primarily relied on perimeter firewalls and routers to protect the intranet, while network-attached components in the experimental hall remained accessible from all internal subnets.

External Stakeholders
When BESSY II became operational, it adopted an open-port approach, enabling user groups to connect complete instrument setups to their designated beamlines. External collaborating research groups (CRGs) were allowed to establish entire beamlines, provided they facilitated shared access with other user groups. This model required support for a Bring Your Own Device (BYOD) framework, introducing external systems and increasing the network complexity within the intranet. The challenge was further exacerbated by the fact that the maintainers of these experimental setups often operated and provided support remotely from their home institutions.

3 Post-Exploit Recovery Measures
The 2023 cyberattack disrupted all IT operations at HZB and BESSY II. Infrastructure isolation contained the incident within 48 hours. Following legal notifications, forensics teams conducted an impact analysis, leading to a three-phase recovery process:

Immediate Response: Non-accelerator systems remained offline until they were thoroughly analyzed, wiped, and reinstalled with event detection and response (EDR) software from a reputable provider. Priority was given to restoring critical business processes and communication systems across the center. A dedicated task force was established to coordinate recovery efforts and facilitate decision-making, with the primary goal of re-establishing the light source user services.

Complex Recovery and Deployments: A new network architecture for the experimental data acquisition IT environment at BESSY II was deemed essential. The migration process, named "ReIP", required all devices reconnecting to the network to undergo proper assignment and integrity certification. ReIP introduced secure zones for accelerators and beamlines, a dedicated development environment for facility controls, and zero-trust zones for user instruments (s. fig. 1). This design minimized the attack surface while incorporating secure connectivity tools, such as jump hosts and EPICS process variable gateways [2]. The implementation involved upgrading, patching, and reintegrating over 50 distinct experiments and managing hundreds of networks and thousands of hosts to enhance cybersecurity.

Creation of Resilient Security Zones: The new environment now implements segmented networks with individual firewalls, strict access controls and independent infrastructure, to ensure data security and uninterrupted beamtime. The initial deployment encompassed 20 servers, 4 clusters, 250 virtual machines (VMs), and 120 networks. Configuration automation via software tools like Ansible or Saltstack now enables "Infrastructure as Code" (IaC) through configuration version control, ensuring consistent deployment and maintenance while minimizing errors. Recovery prioritized core experimental functionalities over non-critical features like remote access, expediting the resumption of data collection for the broader user community.

4 Best Practices Exchange and Intelligence Sharing
HZB engaged a recovery team with expertise in managing cybersecurity incidents for industrial and governmental enterprises. Recognizing the unique challenges of a scientific user facility, the team around

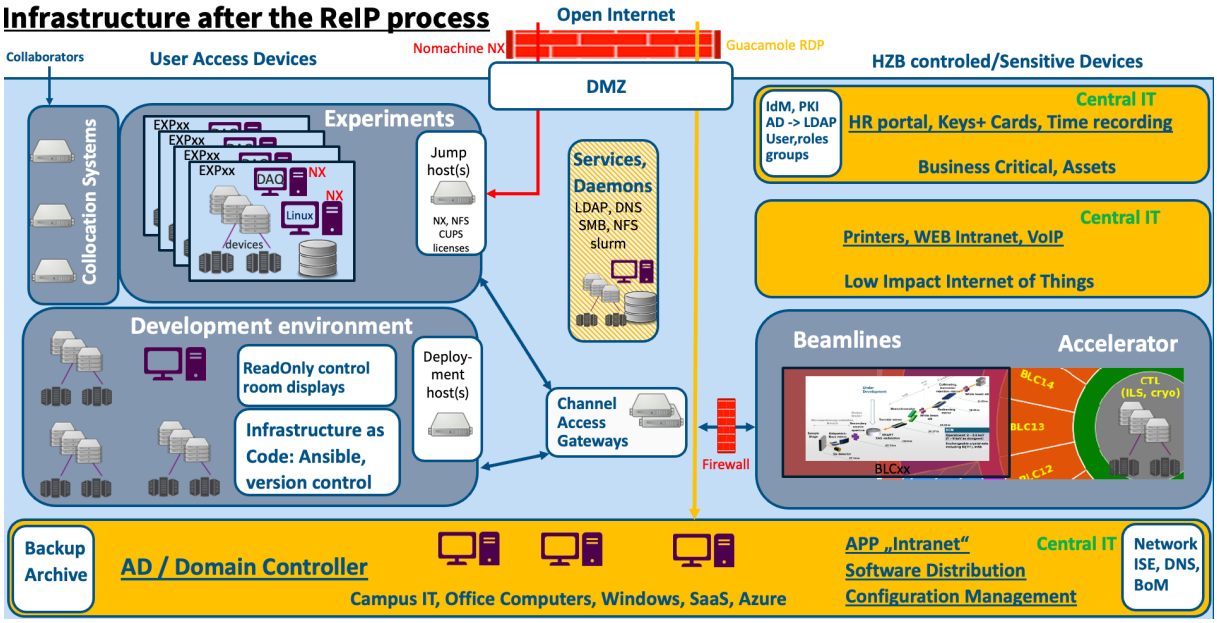

Figure 1: Illustration of the security zones established through the ReIP process for light source operations. Dark grey boxes represent the newly defined zones (Accelerator, Beamlines, Experiments, and Development) utilizing Infrastructure as Code (IaC). Yellow boxes indicate the general-purpose network managed by Active Directory/Domain Controller (AD/DC). The central boxes highlight shared services, including data storage, compute facilities, and specialized network bridges (e.g., Channel Access Gateway).

BESSY II sought expert validation for its recovery plans. To this end, the BESSY II team joined the PaN Cybersecurity Forum, a platform where Chief Information Security Officers (CISOs) from European photon and neutron research infrastructures collaborate to exchange best practices. The forum emphasizes balancing robust security measures with user accessibility, exploring customized solutions to meet research-specific needs. Participants also exchange insights on improving cybersecurity while accommodating external users. With an increasing number of users authenticating through federated identities, the issue of proper identity verification has gained prominence.

5 Prioritization based on NIST Methodology

Following the cyberattack, the primary focus at BESSY II was restoring basic operations. Once instruments were operational and a resilient IT architecture was implemented via the ReIP process, efforts shifted to supporting comprehensive beamtime data management, including remote and automated experiments. Multi-factor authentication (MFA) was promptly deployed and mandated for all external accesses to safeguard against identity theft.

To ensure consistent cybersecurity measures across the facility, a gap analysis was performed. It was guided by the U.S. National Institute of Standards and Technology's (NIST) five key functions "Identify, Protect, Detect, Respond, Recover" [3]. This highlighted the most critical deficiencies, particularly in authentication and authorization processes, as well as in protective network segmentation.

Identity and Asset Management: Identifying abnormal activity requires understanding the baselines: who acts, where, in what role, and with what permissions. This necessitates the definition of roles, policies, and maintenance processes. HZB is currently exploring a unified Identity Management (IdM) system to integrate staff, visitors, and federated identities. From a technical perspective, IdM can utilize a service provision model, linking identity provider databases (IdPs) to service providers (SPs) through SP-IdP proxies (see Fig.2). Proven architectures and open-source federated identity proxies[4, 5] offer reliable solutions for such integration. Effective asset management connects intended use with actual use, as determined by monitoring tools. Intended use is documented within Active Directory or as Infrastructure as Code (IaC). To address supply chain vulnerabilities and mitigate malware risks, a

Software Bill of Materials (SBOM) is also being implemented as a critical component of this approach.

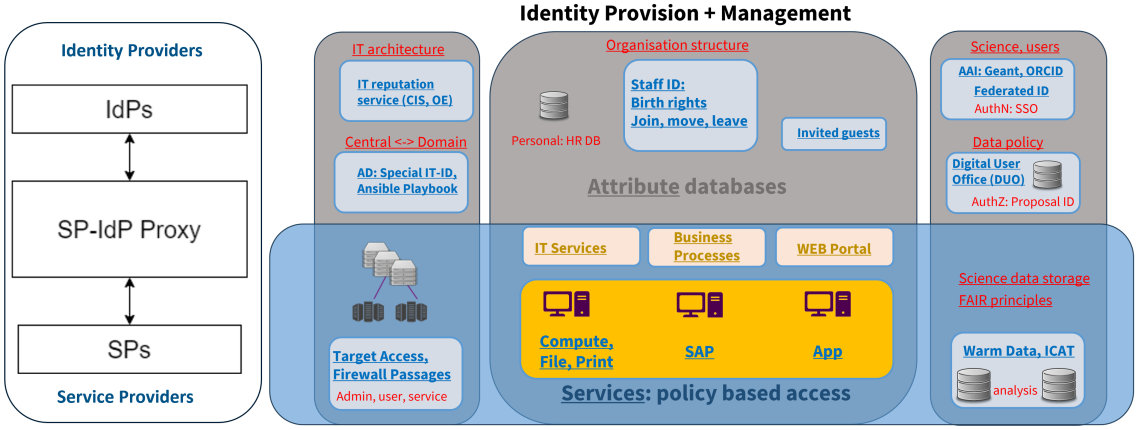

Figure 2: Illustration of identity management requirements at a light source facility. The left box depicts the proxy software principle, connecting identities with services [4]. The right column highlights areas requiring well-defined data access policies, including beamtime users who authenticate to access their acquired data in accordance with the established data policy [6]. The upper middle block represents the attribute databases, detailing the roles, privileges, and responsibilities of individuals operating within HZB's IT environment, including staff, guests, and maintenance personnel, in relation to the center's business processes and IT infrastructure configurations. On the left, the management of IT department privileges is emphasized. The lower blue box underscores that all services function within an interconnected IT infrastructure, necessitating robust cybersecurity measures for effective administration.

Network Security Zoning: The successfully implemented ReIP process must be extended from the large-scale facility BESSY II to the entire HZB in the future. This includes also core laboratories like electron microscopy, material synthesis and characterization setups. Despite the diversity in data management, workflow automation and remote experimentation needs, HZB requires consistent and maintainable security standards. Enhanced firewall and proxy configurations, along with endpoint detection tools such as Carbon Black, are crucial to mitigating risks and ensuring that devices remain secure upon integration. Other ongoing efforts aim to establish an Intrusion Detection or Prevention System (IDS/IPS), with the midterm goal of deploying a Security Information and Event Management (SIEM) system. This SIEM will enable rapid responses to Indicators of Compromise (IoC) and is being refined to enhance its detection capabilities based on lessons learned .

6 Summary

Cybersecurity resilience at large-scale user facilities requires balancing openness, connectivity, and usability with protective measures against adversaries that are neither overly restrictive nor disruptive. The user environment must support unrestricted access to high-end, often cutting-edge scientific instruments, while managing the inherent vulnerabilities of these technologies to cyberthreats. At BESSY II, this balance is achieved through a segmented network architecture: operational systems for the light source are secured within dedicated technical zones, protected by firewalls and role-based access controls. Meanwhile, user instruments are managed within separate zero-trust network zones, reducing the attack surface. This approach ensures a base level of security while preserving researchers' freedom to operate instruments with inherent vulnerabilities, where surveillance remains the primary safeguard.

7 Outlook

A shift in networking architecture paradigms is becoming crucial with the rising data rates of advanced 2D detectors, increased accessibility of machine learning tools on high-performance computing clusters, and the demand for high-speed training data transfers to external centers like the Zuse Institute Berlin (ZIB). Emphasis is needed on transitioning from traditional perimeter-based cybersecurity models to operationalized and interoperable Zero Trust Architecture (ZTA) frameworks. This transition is already advocated in reports such as the Office of Scientific and Technical Information (OSTI) report [7] and other relevant studies.

8 ACKNOWLEDGEMENTS
The authors express their gratitude to all HZB staff members for their valuable and insightful discussions, including contributions from beamline and instrument scientists, accelerator controls, beamline optics specialists, and central IT networking and storage teams. Special appreciation is extended to the members of the PaN Cybersecurity Forum for their constructive feedback and valuable suggestions.

References
[1] (CS2)HEP, Control System CS Workshop series, e.g. https://indico.cern.ch/event/1270052/

[2] https://doi.org/10.18429/JACoW-ICALEPCS2023-TU2BCO04

[3] NIST CSF 2.0 https://doi.org/10.6028/NIST.SP.1271, CIS Critical Security Controls v8

[4] https://aarc-community.org/architecture/

[5] https://unity-idm.eu/ or https://www.scc.kit.edu/dienste/regapp.php

[6] https://www.helmholtz-berlin.de/pubbin/news_seite?nid=14472;sprache=en

[7] Integrated Research Infrastructure Architecture Blueprint Activity (Final Report 2023), Appendix K, p114, https://www.osti.gov/servlets/purl/1984466 or https://doi.org/10.2172/1984466