Case study:

How we improved the IT infrastructure of a medical university, allowing it to collaborate better, both internally & internationally

Part I
Spring 2022

Productivity improvement & security optimization of IT infrastructure

Background

Medical University - Pleven [MU-Pleven] is one of the four major medical universities in Bulgaria. The institution admits hundreds of new students every year, while thousands partake in intensive medical courses.
MU-Pleven is an active member in the global academic exchange via a number of specialized networks focused on faculty, students and medical innovation. In order to conduct these activities efficiently, MU-Pleven needs to improve its overall IT infrastructure and streamline much of its day-to-day work.

Case

MU-Pleven's leadership embarked on a long-term mission to digitalize processes related to the university's faculty management, as well as its core activity - the sharing of medical knowledge among students and peers. As part of the dean's strategic vision, productivity had to be substantially improved via the standardization and unification of processes within the organization. As a secondary goal, data security had to be increased in order to support and protect the newly-found sophistication of its IT infrastructure.

Solution

We began the project with our time-tested GAP analysis. We talked to decision-makers and workers alike, dug deep into the organizational processes, dissected the business goals of the university, and looked carefully at what tactics would be able achieve the client's strategic goals. As always, this included a situational, as well as a risk analysis. The end-product of this preliminary stage was a roadmap, which featured our strategic vision, as well as the concrete stages that had to be passed to attain success.

These stages were:

1. Improvement of IT infrastructure
2. Increase in user productivity
3. Information security

1

Improvement of IT infrastructure: uniform identity

At the onset of the project, there was no centralized identity for users accessing productivity apps within the university's IT infrastructure. Naturally, that ended up being our first objective. We introduced a uniform identity implemented in a dual capacity - an on-premise Microsoft directory founded on physical servers, as well as a cloud-based Azure directory enabling universal authentication. The two domains were synchronized to collaborate seamlessly. Some apps would be based on the university's local servers, while others communicated via the cloud. That decision was made due to legal, as well as practical reasons.

However, the user experience was not impacted by this dual implementation. Employees of the university were now able to log into the various apps using universal credentials. That means that from now teachers and administration of MU-Pleven would be able to access their emails, Wi-Fi, HR, accounting, and other productivity apps via a single identity.

Crucial to this stage of the project was the clien's desire to access eduGAIN. eduGAIN is a network for learning, teaching and data exploitation centered around the use of a single identity. It allows MU-Pleven's faculty to engage in a global knowledge exchange comprised of thousands of medical researchers and practitioners and millions of students. Not only are members of the network allowed to engage with each other, they are also able to do so using uniform credentials. This part of the project was the foundation upon which we built the rest of the infrastructure. The introduction of a single identity solved many organizational problems and paved the way for the next stage - productivity improvement.

0-to-100

single identity incorporation

resulting in ease of access and further capacity acquisition

2

Increase in productivity: organization of labor

Once we finished implementing a single identity for MU-Pleven's employees, we moved onto some housekeeping. The migration of the mail service to the cloud was a big part of that. Our choice for the new cloud-based mail service was Microsoft's Exchange Online - a system that provided a much larger storage capacity, better security and guaranteed access.
Next on our list was the implementation and configuration of SharePoint. Previously, our client used a local environment to collaborate internally, but it was now time to migrate to a much more capable cloud-based intranet. We moved the data from the university's local servers and made sure to utilize SharePoint□s full capability. That meant improved security, more storage and OneDrive integration. The security element of this step cannot be overstated. Universities might not be among the most common targets of malicious activity, but they, too, occasionally fall victim to ransomware attacks.

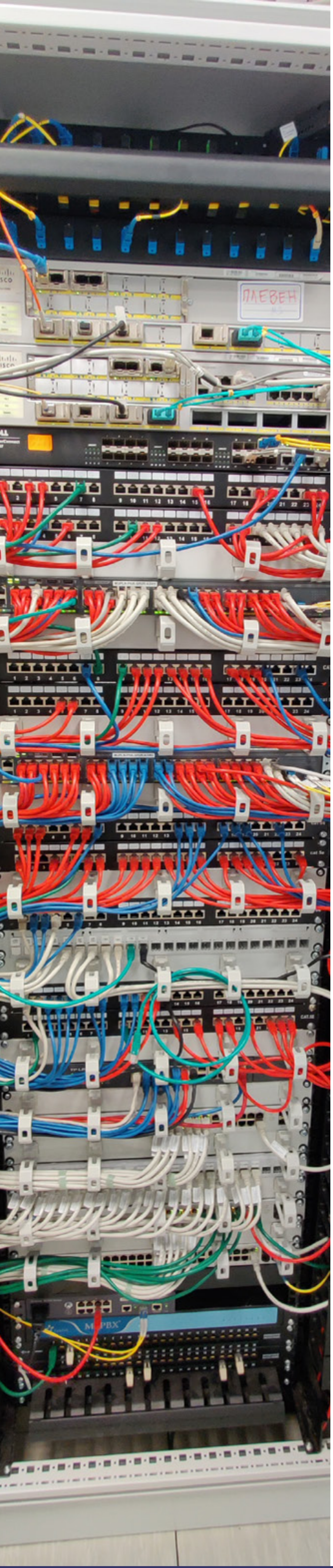
And yet, as important as the improved security was, the biggest change here was the integration of the single identity within the frameworks of Microsoft Teams and Moodle. Since employees of MU-Pleven were now able to log into the various productivity apps using universal credentials, we were able to link MS Teams groups to Moodle resources. We defined dynamic Microsoft 365 user groups and granted them access to specialized data and services via Azure. This enabled a high level of labor organization and collaboration, not least because all information was now securely stored and sharable via Teams and SharePoint.

The end-result? Faculty would now be able to collaborate on teaching resources or academic research using a single identity, while all data is structured, deliberately categorized and safely stored in the cloud. It could be said that the single identity implementation from stage one was only the beginning, while the secure, cloud-based sharing and organization of labor achieved in this stage, was indeed the end goal.

50%

increase in labor productivity

due to cloud-based integration of Microsoft SharePoint, Teams and Office 365



3

Information security: Azure framework

Much of the work on security had already been done at this point. Hosting large parts of the IT infrastructure on Azure meant data security was intrinsic and guaranteed.

But to make sure, we also introduced an Azure data security center, complete with Azure Defender and Azure Sentinel.

These two modules are essential for any large organization dealing with large pools of information, because they provide multiple layers of protection. Two-step authentication, cloud-based backups, real-time monitoring and reporting, as well as AI-powered security analytics, are just a few of the features that come into play here.

100%

improvement

of IT security due to implementation of Azure infrastructure, including Defender & Sentinel

Conclusion

MU-Pleven's project was a classic example of capacity building and how MY Synergy approaches this challenge. We had a structured approach - a roadmap resulting from a GAP analysis emphasizing continuity. Introducing a single identity [stage 1] led to expanded opportunities. Once realized, those extra features improved the institution's overall productivity [stage 2].

IT solutions are meant to service business goals and should not exist in and of themselves. By incorporating the necessary infrastructure, we increased the level of cooperation within the organization and its capacity to collaborate with external partners.

Visit our website for more solutions

Our community: