



Czech Ministry of Finance: Securing the Nation's Critical IT from Active International Cyber Threats

The Ministry of Finance is responsible for the financial health of the Czech Republic. Administrating the state budget and treasury, collecting taxes, and regulating financial and capital markets are just some of the ministry's critical functions. With cyberattacks on the nation's public institutions on the rise, particularly highly sophisticated attacks launched by foreign intelligence agencies, the ministry's IT systems needed to be further protected against the ongoing threats.

That's why the Ministry of Finance State Treasury System, which is responsible for state budget planning and expenditure control, was declared a "critical IT system" according to the Czech Republic's Cyber Security Act. It's also why the Ministry needs **a trusted technology partner** to introduce new security measures and tools to fully protect sensitive data and critical government processes operated in the information system.



Achieving Next-Level Cybersecurity for the Czech Republic's State Treasury System using **SAP® Solutions and Services**



Before: Challenges and Opportunities

- Secure the State Treasury Information System critical to national security and government operations
- Defend against a rise in sophisticated cyberattacks launched against public interfaces of the system
- Establish a complete, integrated cybersecurity approach that adapts rapidly to new threats

Why SAP and IBM Česká Republika, spol. s r.o.

- Security solution and best-practice implementation expertise from SAP Advisory Services
- Solutions for all aspects of cybersecurity – from access control to vulnerability and threat detection
- System integration and high-level project management services provided by IBM Česká Republika to ensure compliance with the Ministry's overall security blueprint

After: Value-Driven Results

- Rapid response to cyberattacks on SAP software using the SAP Enterprise Threat Detection application
- Infrastructure security to prevent data leaks and internal fraud using SAP governance, risk, and compliance solutions
- Improved productivity and reduced username and password leaks with the SAP Single Sign-On application
- Custom code quality checks and security verification using the SAP Code Vulnerability Analyzer tool

“We are pleased that we could rely on the best practices and expertise of SAP Advisory Services to implement our security software for the State Treasury Information System. Now, our cybersecurity is **strengthened and fully compliant** with the Cyber Security Act.”

Jan Áčko, Head of the State Treasury System, Ministry of Finance

Constant

Security level improvement

Active

Cyberattack detection and response

Featured Partner



Ministry of Finance
Prague, Czech Republic
www.mfcr.cz

Industry
Public sector

Products and Services
Finance administration including state budget, treasury, and taxation

Employees
1,450

Featured Solutions and Services
SAP Advisory Services, SAP Enterprise Threat Detection, SAP Access Control, SAP Single Sign-On, and SAP Code Vulnerability Analyzer

THE BEST RUN 

Follow us



www.sap.com/contactsap

Studio SAP | 71871enUS (20/11)

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/copyright for additional trademark information and notices.