BANCA NAȚIONALĂ A ROMÂNIEI

Mastering Cybersecurity in the user mindset

Cybersecurity / IT Risk

National Bank of Romania
Gerald Dinca

September 2020

COVID-19 Impact in Romania

The extent of the pandemic, impact on the economy

- Romania's economy will shrink in 2020 by 5-6%
- 50% of the most important companies in the country were already facing difficulties (approx. 29,000 companies that have assets of over 1 million euros)
- the average number of employees in the economy is forecast to decrease by 1.6%

Key challenges the financial sector faces

- decreasing the number of operations intermediated
- decreasing in the number of investments – "..Investors will not finance a budget deficit out of control.." (according to Mr. Cristian Popa, NBR Board member)

How has financial institutions' operations changed in response?

- accelerated digitization in relation with the customers;
- remote work for more that 50% of the employees (starting from almost 0%);
- Protective measures for both customers and employees.

Theory vs. Reality in Cybersecurity

Theory

- We are prepared for any crisis that may come;
- Our user's reaction could be anticipated;
- An optimistic mindset will not only help overcome the adversity and fare through the storm but it may also lead to positive outcomes through innovation and resilience.

Reality

Most organizations are currently dealing with a situation NEVER BEFORE realized for a remote workforce:

- Secure access;
- Provisioning;
- Hardware;
- Authentication;
- Support;
- And THE USER MINDSET (never been before in this situation).

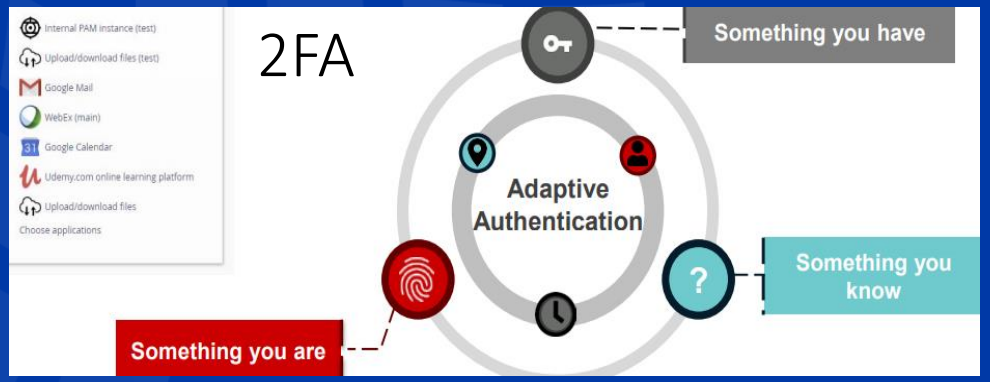
Risks vs. Controls

Due to massive increase in use of SaaS apps (WebEx, MS Teams, Zoom etc.), we have to deal with the following RISKS:

- Weak passwords, possibly already shared and compromised;
- Lack of a culture regarding 2FA;
- Bring Your Own Device concept;
- Lack of a procedure for fast acquisition of mobile infrastructure.

CONTROLS:

- Identity Access Management platform:
  - Strong passwords and synchronization;
  - Adaptive, MFA and federation;
  - Privileged access management;
  - Audit and reporting standards.
- Synchronize passwords across applications:
  - Reduce the number of passwords
- Enforce a consistent password policy



Outlook

Plans for the future for Financial Supervision in general and Cybersecurity / IT Risk Supervision in particular

- a common framework for Penetration testing activities;
- adapting the business continuity plans according to the new challenges

Expectations from financial institutions regarding the Cybersecurity threats

- increasing the level of user awareness
- increasing the remote work usage covered by modern and secure platforms
- Implementation of specific tools for Security Orchestration, Automation, and Response
- Join to the Cybersecurity Community in order to properly respond to the newest Cybersecurity threats.

“Cyber Security is a Shared Responsibility”