SCHNEIDER GROUP

IT-solutions for Information Security

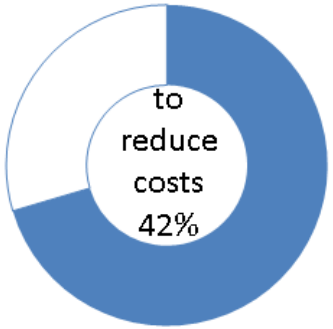
Thomas Titsch
Director ERP, SCHNEIDER GROUP
Cyber Security Forum
February 9, 2016 – Digital October

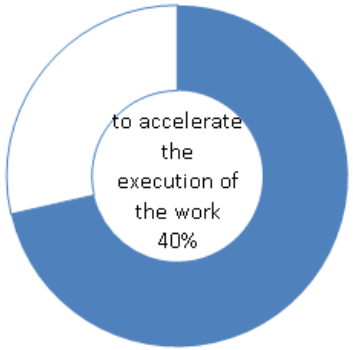
Agenda

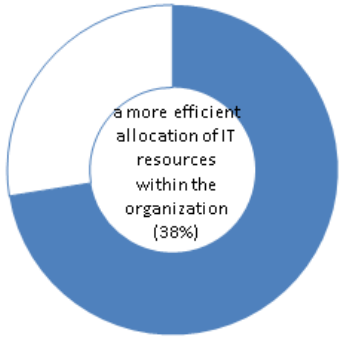
- 1C safety functions and Cloud Solutions
- Information security requirements for SaaS-applications
- How to choose a reliable SaaS provider
- How to avoid security breaches

1C safety functions and Cloud Solutions

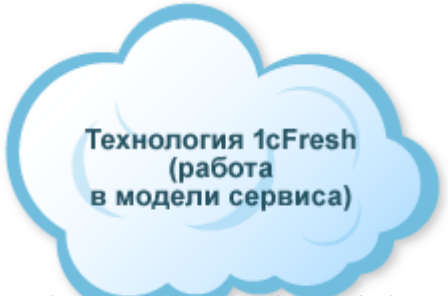
- The Russian market of cloud services for small and medium-sized companies rose by more than 4-fold, to 88 billion rubles for the last 2 years
- The use of cloud solutions helps:





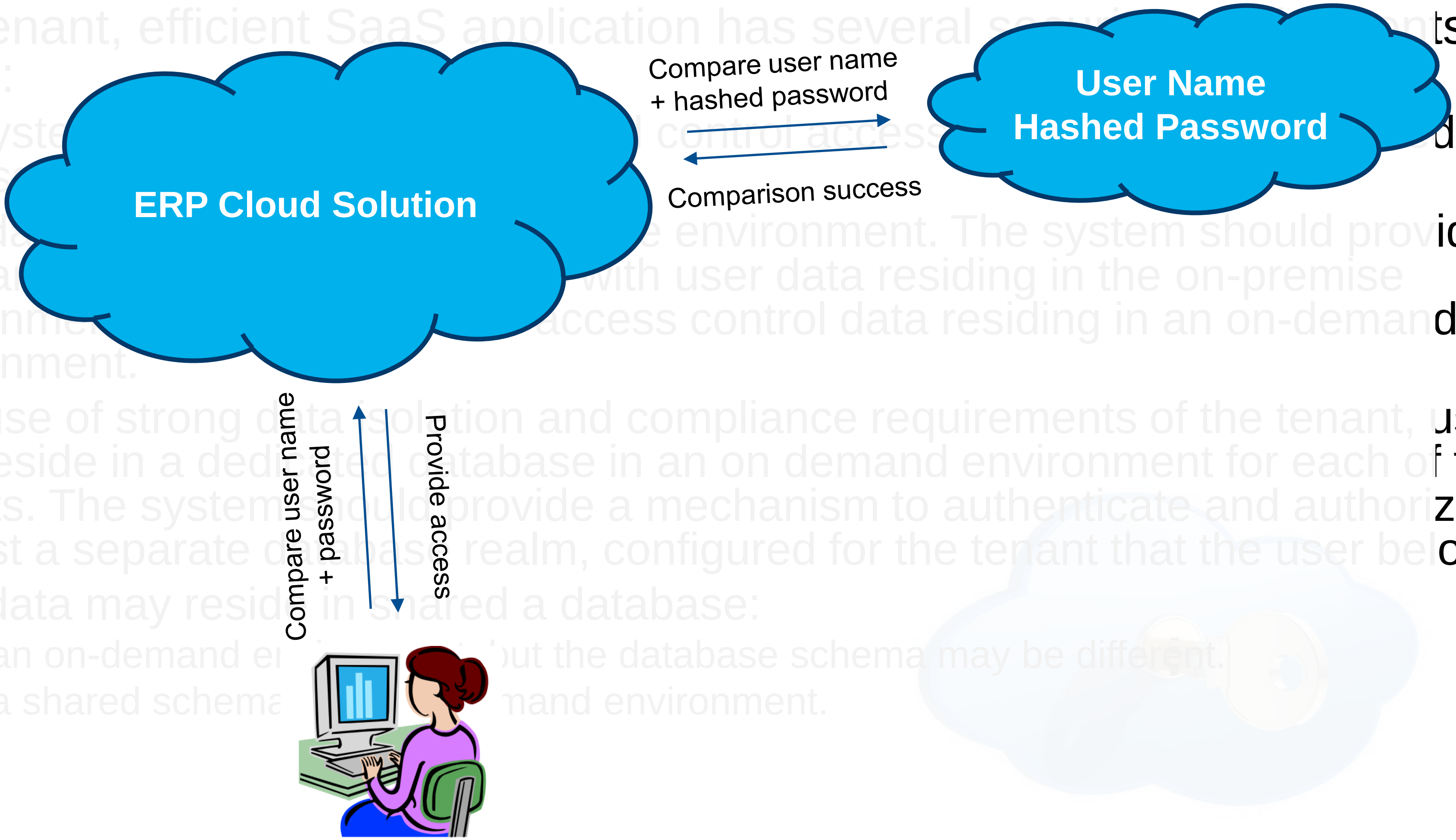


- The company "1C", the largest manufacturer of business applications in Russia, outlined its strategy for the development of business in the clouds - Software as a Service (SaaS)



Information security requirements for SaaS-applications

- A multi-tenant, efficient SaaS application has several s… ts including:
  - The syste… control access … d on perm…
  - User d… e environment. The system should provide mech… with user data residing in the on-premise environment … access control data residing in an on-demand environment.
  - Because of strong data isolation and compliance requirements of the tenant, user data may reside in a dedicated database in an on demand environment for each of the tenants. The system should provide a mechanism to authenticate and authorize users against a separate database realm, configured for the tenant that the user belongs to.
  - User data may reside in shared a database:
    - In an on-demand e… but the database schema may be different.
    - In a shared schema … mand environment.

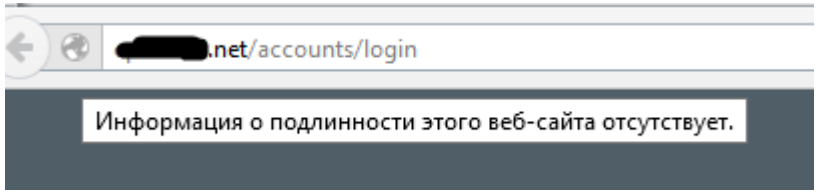


How to choose a reliable SaaS provider

- SaaS provider should organize the following security measures is to avoid negative impact on the company's business processes, increase efficiency and stable profit from SaaS use:
  - for right choice of provider must be fully familiar with the contract of service, especially the section relating to the duties of the operator data protection of its client companies
  - the ability to use the most advanced encryption system to meet the current IT security issues
  - the presence of two-factor authentication, control of both the rights of users, as well as prompt and timely cancellation of lost information
  - the ability to use a log event (Monitoring)
  - the ability to carry out security checks

How to avoid security breaches

- Do not use a shared database with other companies.
  - "1C" bring to the attention of customers and partners, which in version 8.3.6 platform "1C: Enterprise" has encountered a problem: in some rare cases, improperly defined permissions on a record level.
- Do not use unencrypted communication channels
  - For a example



- Do not use to encrypt communication channels SSL 3.0 [RFC 6101] - it is outdated and insecure protocol
- Use Remote Desktop Protocol (RDP) ALWAYS with last updates

omas Titsch
ector
schT@schneider-group.com

SCHNEIDER GROUP

russia
ukraine
belarus
kazakhstan
germany
poland

accounting | erp | import | legal | tax

www.schneider-group.com