**#tinkoff fintech**

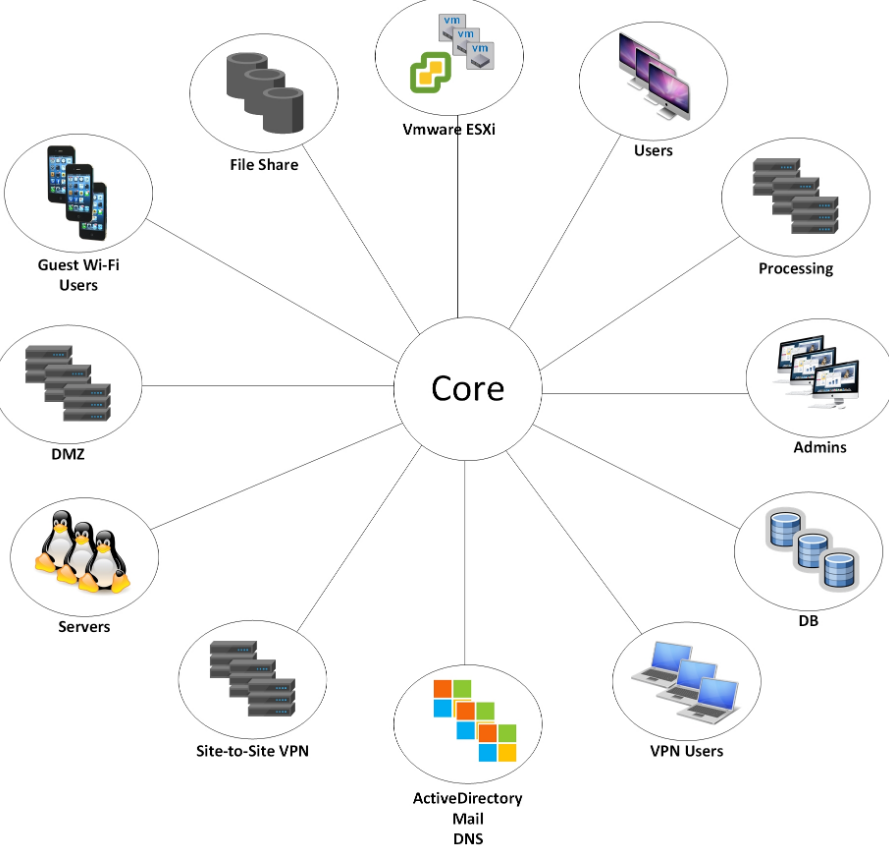
homework #5

**BANK**   
SECURITY CHALLENGES

**08.04.2019**

# Задачи:

1. **Составить матрицу угроз для типовой схемы организации**

****

### Введение.

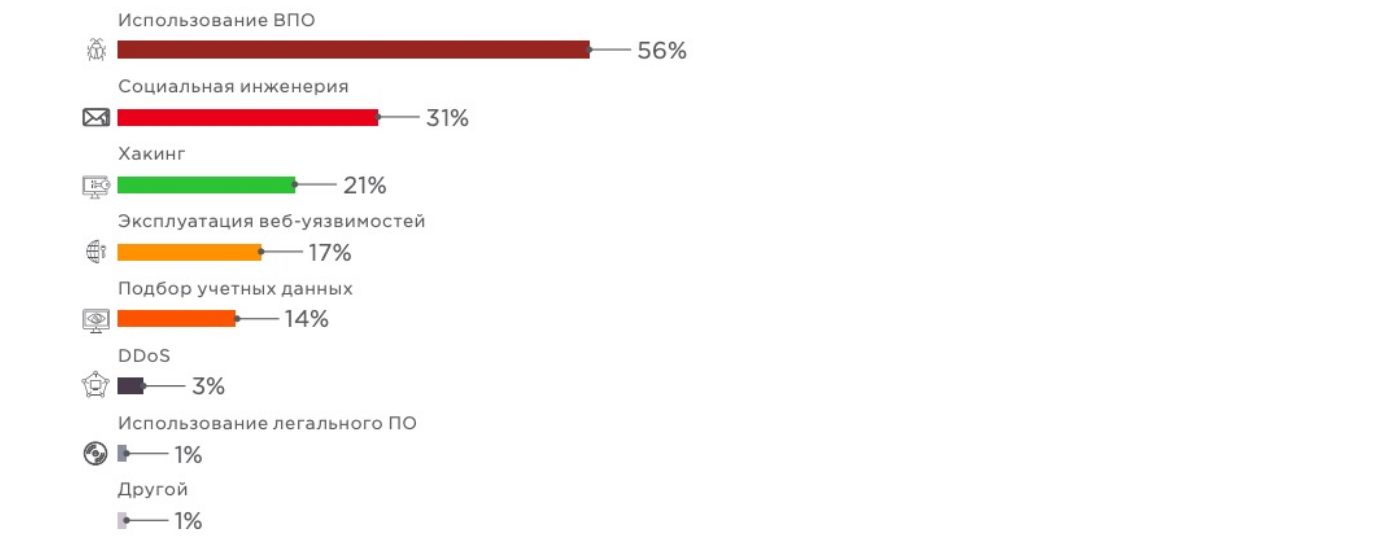
Согласно статистике за 2018 год, проведенной компанией Positive Technology **самым атакуемым объектом** является инфраструктура банка, затем веб-ресурсы и пользователи.



К инфраструктуре банка следует отнести такие объекты как: **Servers, DB, DMZ, admins, users, processing, AD and email / DNS, file share, vmware, guest wifi users,**  **etc**.

В первую очередь, надо понимать, что поскольку атаки на инфраструктуру многочисленны, современные банки имеют достаточно эффективные барьеры для защиты от внешних угроз. Поэтому в настоящее время, наиболее опасными для банков с secure by design архитектурой, являются атаки на основе социальной инженерии**,** направленная в основном на **sending phishing emails to employees.**

По методам атаки есть хорошая наглядная статистика от PT:



Теперь чуть подробнее по угрозам / методам защиты сегментов.

### 

### 1. Segment - SERVER

## Threats:

* WEAK PASSWORD (капслок, потому что проблема очень актуальна).
* Old version of software (possible to be exploited, not secure)
* Misconfiguration (open ports, unused services, etc)
* Denial-of-service attack
* Human factors (халатность, невнимательность, недостаточно подготовленный персонал).

## Countermeasures:

* Advanced password policy (require strong secure password)
* Upgrade software ()
* Hardening Guides & Patch and Vulnerability management (using tools like **NESSUS**)
* NGFW (next-gen fw)
* ACL

***Recommendation: Seriously, stop using weak passwords. Although, do regular scans for vulnerabilities. Watch for zero-day’s attacks.***

### 2. Segment - DB (almost the same threats as server)

## Threats:

* WEAK PASSWORD (капслок, потому что проблема очень актуальна).
* Old version of software (possible to be exploited, not secure)
* Misconfiguration (open ports, unused services, etc)
* Not secure access policy
* Human factors (халатность, невнимательность, недостаточно подготовленный персонал).

## Countermeasures:

* Advanced password policy (require strong secure password)
* ACL
* Upgrade software ()
* Advanced Access Policy
* Hardening Guides & Patch and Vulnerability management (using tools like **NESSUS**)
* NGFW (next-gen fw)

***Recommendation: Store sensitive information with encryption.***

### 3. Segment - DMZ

## Threats:

* Web vulnerabilities
* Old versions
* Bad password hygiene :)
* Direct access to DB network (permissive access control)
* Insufficient Logging & Monitoring
* Lack of segmentation

## Countermeasures:

* Security by Design
* WAF
* Hardening Guides
* Patch and Vulnerability management
* ACL & FW

***Main idea: Prevent a network security attack by isolating the infrastructure***

### 4. Segment - Admins

## Threats:

* Not following security policy (халатность, невнимательность, самоуверенность)
* Social engineering
* Viirus
* Layoff (убедиться что у сотрудников нету доступа к корпоративной информации)

## Countermeasures:

* Start following security policy :)
* Take part in some IT-sec courses
* Antivirus
* Trying to not make SUPER admins if it is not needed
* Layoff (убедиться что у сотрудников нету доступа к корпоративной информации)

***Main idea: Hire professionals or make them (by attending IT-courses, etc)***

### 5. Segment - USERS

## Threats:

* Not following security policy / Lack of professional skills (халатность, невнимательность, самоуверенность)
* Social engineering
* Viruses
* Layoff (убедиться что у сотрудников нету доступа к корпоративной информации)

## Countermeasures:

* Start following security policy :)
* Take part in some IT-sec courses
* Antivirus
* Layoff (убедиться что у сотрудников нету доступа к корпоративной информации)

***Main idea: Hire professionals or make them (by attending IT-courses, etc)***

### 6. Segment - AD and email / DNS

## Threats:

* FISHING (caps because it is the most common one)
* Spoofing / Sniffing

## Countermeasures:

* Antivirus
* Sandboxing
* Improving overall knowledge in Cybersec area

***Main idea: Use sandboxing. Antivirus. Brain. (not exactly in this order :))***

### 

### 7. Segment - VMWARE

## Threats:

* DoS-attacks
* Hypervisor exploits aka VM Jumping (user logged into one VM can hop over to another VM)
* Network threats
* Каналы связи между хостовой и виртуальной машины (guest addition)
* Host Traffic Interception (tracking of system calls, paging files, memory)

## Countermeasures:

* Security best practices aka Hardening Guide (correct usage of built-in security features as well as additional security measures, such as Limit access, Do not access managed hosts directly, Use DCUI only for troubleshooting)

# info found on official site of vmware: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.security.doc/GUID-B39474AF-6778-499A-B8AB-E973BE6D4899.html>

***Main idea: At least do some basic hardening guide and apply traditional security approaches. Although, beware of zero-day’s attacks, coz virtualisation is still in “early-stage” and could be potentially prone to some new exploits***

### 8. Segment - PROCESSING

## Threats:

* Most of the threats are common with Server segment (ACL / Firewall /NGFW)
* Absence of two-factor authentication for access to critical systems
* Lack of monitoring and logging system events.
* Control input / output money processing.

## Countermeasures:

* Security best practices aka Hardening Guide
* Two-factor authentication. Improving security policies. Access only by specific IP address.
* Integrity controls
* Professional stuff

***Main idea: Hire professionals or make them (by attending IT-courses, etc)***

### 9. Segment - FILE SHARING

## Threats:

* Viruses (any kind of them)
* Using 3rd party cloud services (no control over data due to storing files usually outside of company). Although potentially DATA LEAKAGE
* BYOD aka “Bring Your Own Device”
* Using outdated Software (as well as Misconfiguration)

## Countermeasures:

* Antivirus / NGFW
* Don’t use third party services
* File system permissions (do some chmod-ing :))
* Patch management
* Hardening guide

***Main idea: File sharing policy. NGFW. Don’t use 3rd party cloud services especial for sensitive information.***

### 

### 10. Segment - GUEST WIFI USERS

## Threats:

* Unencrypted connection (possible to sniffing)
* Wireless attacks
* Don’t use WIFI for sensitive information

## Countermeasures:

* Encrypted connection with WPA2 / PSK + RADIUS server
* Improving overall knowledge in Cybersec area

***Main idea: If possible don’t use wifi for sensitive information.***