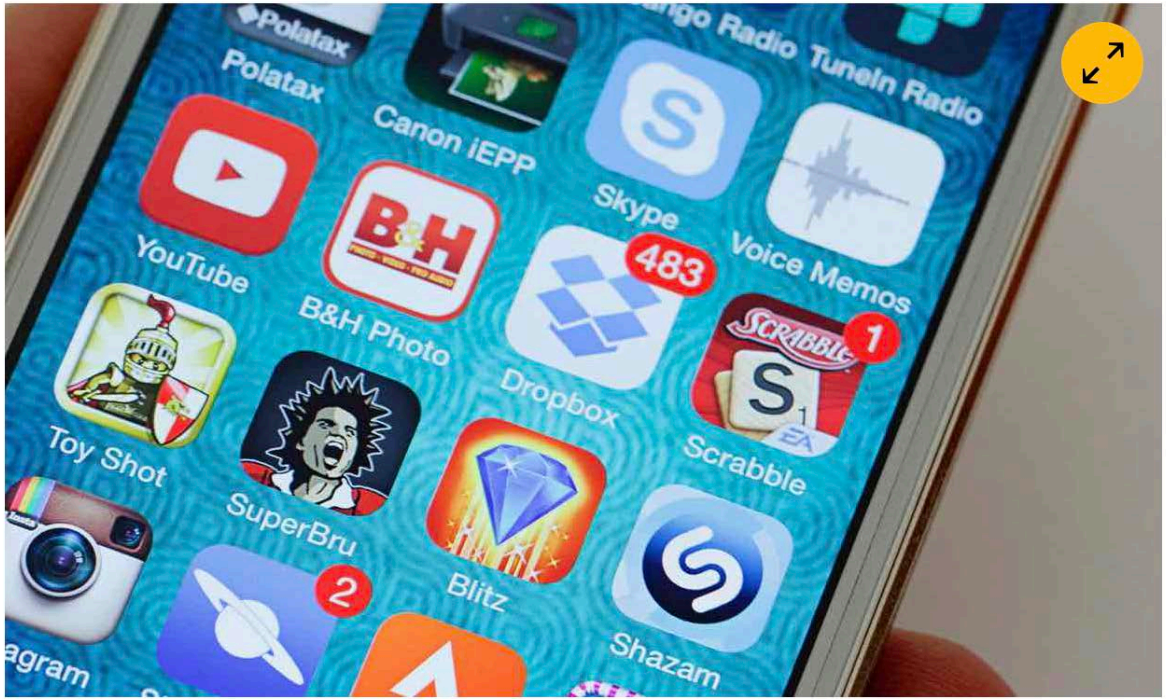
Security risks in the public cloud and how to dispatch them

Men Beglinger
Manager Datacenter Management

accelerIS
and IT works

Dropbox hack leads to leaking of 68m user passwords on the internet

Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked



The Dropbox data breach has highlighted the problem of password reuse. Photograph: Alamy

Yahoo's hack warning comes from third breach, the company says

Michelle Castillo | @mishcastillo
Wednesday, 15 Feb 2017 | 1:38 PM ET

AP

CNBC

https://en.wikipedia.org/wiki/Yahoo!_data_breaches

From http://verelox.com/

First of all, we want to offer our apologies for any inconvenience.

Unfortunately, an ex administrator has deleted all customer data and wiped most servers.
Because of this, we took the necessary steps to temporarily take our network offline.
We have been working hard to recover the data but this was not possible for all data that was lost.

Our network and hosting services will be back this week with security updates.
Current customers who are still interested in our services will receive compensation for their services.
If clients have important data please contact us at support@verelox.com.
We will try our best with our technical team to recover you data.

Security Threats

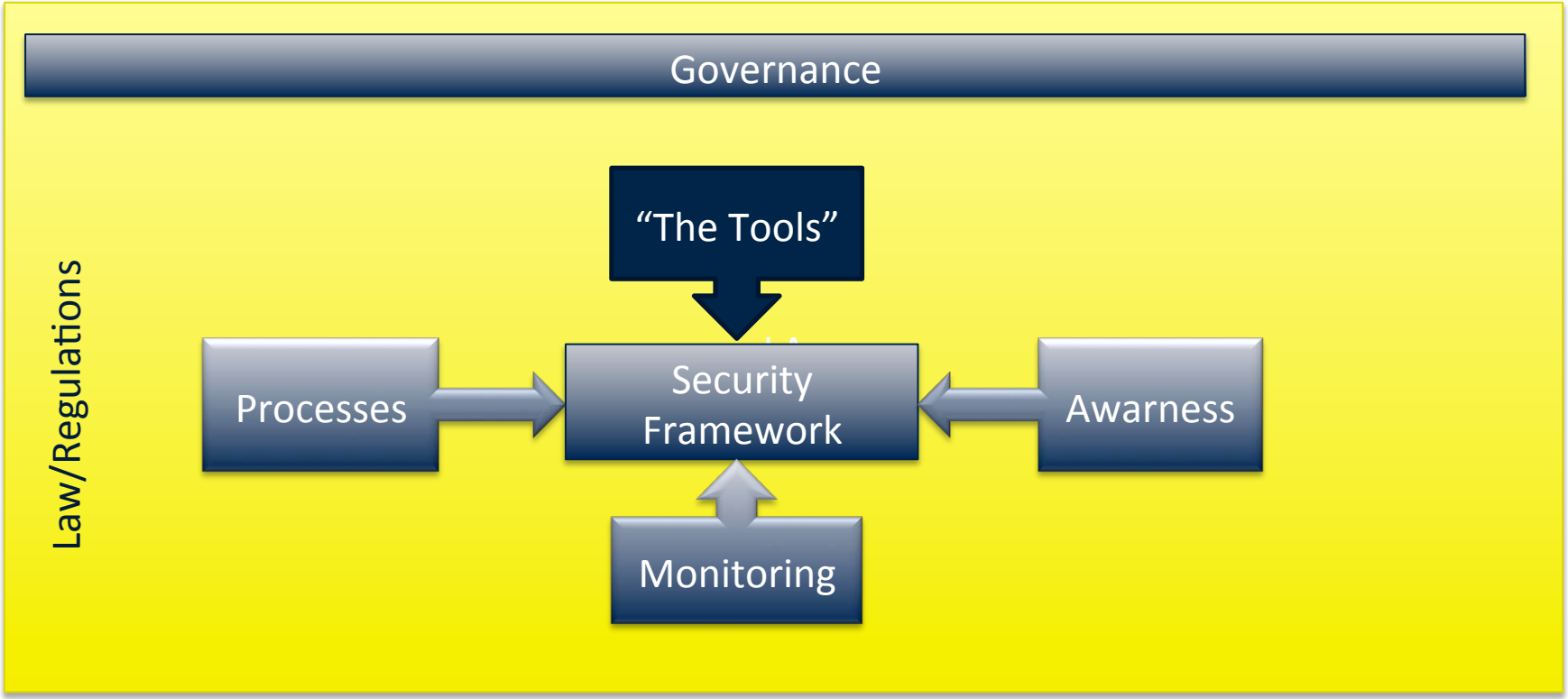
- The most common threats of Cloud Platforms, according to several sources in the internet:
  - Data Breach
  - Data Loss
  - Account or Service Traffic Hijacking
  - Insecure API's
  - Denial of Service
  - Malicious Insider
  - Abuse of Cloud Services
  - Insufficient Due Diligence
  - Shared Technology
  - Malware/Virus/Phishing
  - APT's (Advanced Persistent Threats)

Whats the diff. between public clouds and private cloud?

- Private Clouds only have a few entry points from the internet
  - Mail, Websites, few Applications
  - VPN
- The possible damage is limited to one company
- The amount of data is limited and probably not that interesting
- Access to public services can be limited (f.e only from europe)
- The workload is known and can be monitored

- From a technical point of view: No real difference. But in real live a public cloud provider is a worthwhile goal

Security Framework



The Tools

- Configuration Management
- Identity Management
- Encryption
- One Time Password
- Firewall
- Logging
- Monitoring
- Mandatory Access Control (SELinux)
- sFlow
- Anti Virus Solution
- …

Most common threats

Threat	Risk Level	Mitigation
Data Breach	5	IdM, Encryption,SELinux
Data Loss	5	Backup, SELinux
Compromised Credentials	6	IdM, OTP, SELinux
Insecure API's	6	FW, Logging
Denial of Service	4	BGP, dual ISP,
Malicious Insider	4	SELinux,IdM,Logging
Abuse of Cloud Services	3	Logging, Monitoring
Insufficient Due Diligence	2	
Shared Technology	6	SELinux, Logging, File integrity monitoring
Malware/Virus/Phishing	8	Monitoring, Logging, Anti Virus
APT's	8	sFlow, Monitoring, Logging

Malware/Virus/Phishing

- These threats are mostly introduced by employees or customers
- The threat factor has increased by time and will still increase to the future
- Keep the awareness of customers/employees as high as possible

- Use a mail gateway with malware/virus/phishing detection
- Introduce a central managed virus/malware detection and prevention
- Create regular backups of the data

APT’s

- APT’s (advanced persistent threat) is a newer form of threat
- They try to get a foothold in the infrastructure and then start slowly to gather information's and steal data
- They are really hard to detect – one of they’re primary goals is to stay as long as possible in place

- Check Network for unusual traffic
- Use Malware protection on threatened systems

Compromised Credentials

- Compromised credentials are a huge risk for customers and service providers
- This affects also the application passwords

- Implement two factor authentication for Administrative Users
- Give the customers the possibility to migrate to two factor auth.
- Force a certain level of password complexity (not too high…)

Insecure API’s

- API’s are the “key” to access cloud services
- They are used to manage the whole cloud environment
- Access to the Cloud API with admin privileges is worst case!

- Make sure that the API version is up2date
- Protect the API as good as possible with the firewall
- Trace and log the calls to the API (..and analyze them!)

Shared Technologies

- Cloud platforms are efficient in sharing resources, but this can also lead to risks
- A single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud
- Encrypted auth (no plain text auth for FTP/SMTP/HTTP/etc)
- Role/Privilege separation
- Encryption of data/communication
- Logging / Audit
- Mandatory Access Control
- File Integrity Monitor at root level of the services (tripwire, aide etc)
- Intrusion Detection (processes, open/used ports)

Don’t forget the rest

- Not only the technical mitigation is important
- Have your documentation ready and up to date
- Manage your processes and improve them
- Keep the awareness of employees and customer as high as possible
- **Be prepared – expect the best but prepare for the worst**

General Data Protection Regulation (GDPR)

accelerIS
and IT works

LEGAL DEADLINES OF THE GDPR

- Entry into force on May 24th 2016
- But two-year **transition period**
- After expiry of this deadline, it will be applied without exception from **May 25th 2018!**

APPLICABILITY OF THE EU GDPR

- GDPR not only applicable to EU companies
  → Larger territorial scope

- Also **non-EU** companies **willl be covered** by the GDPR!

- 2 **exceptions**:
  - non-appliability if data controller, processor and data subject are all based in CH
  - partial applicability if data subject is based in EU, data controller or processor are based in CH
    → Applicable where data processing activities are related to (1) the offering of goods or services or (2) monitoring of data subject's behavior.

PRINCIPLES AND CHARACTERISTICS OF THE EU GDPR

- **Violations** get **penalized** drastically!
  - **4%** of the worldwide turnover or **EUR 20 Millions** (whichever is higher)

- Mandatory **reporting** of data breaches
  - within **72 hours** to the supervisory authority
  - if present **high risk immediately** to the data subjects concerned

PRINCIPLES AND CHARACTERISTICS OF THE EU GDPR

- "**Enterprise**" in the sense of GDPR
  - **Irrespective** of its legal form (SA/AG; Sàrl/GmbH; branch or subsidiary with legal personality)

- Conditions for **consent** of processing personal data
  - Data controller shall be able to **demonstrate** the given consent
  - Request for consent shall be presented in a **clear** and **easily understanding** manner
  - Data subject has the right to **withdraw** consent **at any time**
  - To withdraw consent shall be **as easy** as to give consent

PRINCIPLES AND CHARACTERISTICS OF THE EU GDPR

- **Controller** has to **inform** the data subject about data processing in a **transparent** and **easily accessible** form, using **clear** and **plain** language
  - long list of information to be provided where personal data is collected

- High **increase** in **rights** of the affected person (data subject)!

- Controller shall **facilitate** the exercise of data subject rights

Revision of the Swiss Data Protection Act (LPD/DSG)

accelerис
and IT works

REVISION OF THE SWISS DATA PROTECTION ACT (LPD/DSG)

- **Preliminary draft of the new act**
  - Has been in consultation procedure till April 4th 2017
- **Clear orientation to the new EU GDPR**
  - Higher sanctions
  - Privacy by design
  - Notification of data breaches
  - Assessments prior to actions
- **Right of access to the processing of personal data**
- **Fine up to CHF 500‘000.-**
- **Strengthening of the supervisory authority (EDÖB)**

Contact information

Men Beglinger

Manager Datacenter Management

Tel. +41 79 208 69 13

men.beglinger@acceleris.ch