From 0 to Secure in 1 Minute

APPSEC IL 2015

Moshe Ferber
CCSK, CCSP
#About

- Information security professional for over 20 years
- Popular industry speaker & lecturer (DefCon, BlackHat, Infosec and more)
- Co-Contributor for CCSK, CCSP and other cloud security initiative.
- Founded Cloud7, Managed Security Services provider (currently 2bsecure cloud services)
- Partner at Clarisite – *Your customer’s eye view*
- Partner at FortyCloud – *Make your public cloud private*
- Member of the board at Macshava Tova – *Narrowing societal gaps*
- Certified CCSK instructor for the Cloud Security Alliance.
- Certified CCSP instructor for ISC2.
- Co-Chairman of the Board, Cloud Security Alliance, Israeli Chapter
About the Cloud Security Alliance

- Global, not-for-profit organization
- Building security best practices for next generation IT
- Research and Educational Programs
- Cloud providers & security professionals Certifications
- Awareness and Marketing
- The globally authoritative source for Trust in the Cloud

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing”

CSA Israel: Community of security professional promoting responsible cloud adoption.
About the talk

Cloud security challenges and benefits
And more specifically, using IaaS automation and orchestration features for increasing the security

Dashboard
Billing
API
Orchestration
Hypervisor
Controller
Abstraction
Physical Servers
Network
Storage
About the talk

Cloud Attack Vectors

- Provider administration
- Insecure instances
- Management console
- Side channel attack
- Multi tenancy & virtualization
- Chain of supply
- Automation & API
Anatomy of a cloud hack
Anatomy of a cloud hack – the BrowserStack story

- Shell shock vulnerability on unused server
- Found API key on hacked server
- Using API key opened a firewall rule and launch an instance
- Attached a backup volume to the instance
- Found database credential on backup device
- Connected to DB

SOURCE: https://www.browserstack.com/attack-and-downtime-on-9-November
Do we have the right tools?

Architecture & Deployments is changing

AUTO SCALING

Micro-Services Architecture

DEV  OPS

Continuous Delivery

The billing cycle is reducing

Google slashes cloud platform price again

Microsoft will offer Azure by the minute to take on Amazon’s cloud

Microsoft follows Google with by-the-minute cloud blending

1 hour

10 min

1 min
How to do security when servers alive for 10 minutes?

- Patch management
- Maintenance windows
- Periodic vulnerability scanning
- Hardening
DON’T LET SECURITY HOLD YOU DOWN

Source: www.avon-barrier.co.uk
Introducing

SOURCE: http://www.cloudefigo.org/

Based on the work made by Rich Mogull from Securosis
https://github.com/securosis
Cloudefigo Lifecycle

1. Server launch
2. Server loads security configuration
3. Server encrypts disk volumes
4. Server scanned for vulnerabilities
5. Server moves to production
Components

- Object Storage
- Vulnerability Scanner
- Cloud-Init
- Configuration Management
- IAM Roles
- Volume Encryption
Instant Lifecycle

- Launch
- Update
- Control
- Scan
- Terminate
- Production
Wrapping Up

The new software architecture and applications delivery in cloud module disrupts traditional correctives controls.

We need to adopt new thinking to automate security.

Think how security automation can help you in moving your infrastructure forward. Faster.
Questions

Moshe Ferber
@: moshe (at) onlinecloudsec.com
w: www.onlinecloudsec.com
in: www.linkedin.com/in/MosheFerber
t: @FerberMoshe