Let’s rethink cloud application security in 2016
About me

Patrick Kerpan
CEO at Cohesive Networks
@pjktech
About Cohesive Networks

- 2,000+ customers protect cloud-based applications
- User-controlled security & connectivity at the top of the cloud
- Cloud is creating demand for more connectivity and security

honest approach to cloud security
Agenda

• data center security is not cloud security
• post-Snowden realities
• application layer network security
• upcoming security compliance regulations
• here’s to a more secure 2016
data center security is not cloud security
modern apps

Database Tier

AppServer Tier

Web Tier

business applications are collections of servers
enterprise data center

enterprise data centers are filled with these applications
80% of security spend is on perimeter, leaving only 20% for interior network security
data center vulnerability

Perimeter Security

Hacker Penetration
data center vulnerability

Vulnerabilities go undetected for an average of 234 days!
post-Snowden realities
target: governments

Panama Papers fallout: Iceland's Prime Minister resigns

By Tim Hume and Zoe Robert, CNN
Updated 12:39 PM ET, Tue April 5, 2016 | Video Source: CNN

Reykjavik, Iceland (CNN) — The Panama Papers leaks apparently resulted in a political casualty Tuesday when Icelandic Prime Minister Sigmundur David Gunnlaugsson resigned.

Sigmundur Ingjaldsson, the deputy chair of the Progressive Party, announced Gunnlaugsson’s resignation Tuesday on Iceland’s national public service broadcaster.
Target CEO resigns after data breach fallout

Gregg Steinhafel steps down in wake of a hack last December that affected as many as 110 million Target customers.
Anthem data breach cost likely to smash $100 million barrier

The company’s cyber insurance policy is likely to be exhausted following the theft of up to 80 million records.

By Charlie Osborne for Zero Day | February 12, 2015 -- 12:54 GMT (04:54 PST) | Topic: Security

The financial consequences of Anthem’s massive data breach could reach beyond the $100 million mark, according to reports.

The US health insurance provider’s cyber insurance policy, led by the American International Group, covers losses of up to $200 million. However, when a company has up to 80 million current and previous customers, staff and investors to contact, reassure and notify, this amount may not be enough.

Last week, Anthem confirmed a security breach which resulted in the exposure and theft of up to 80 million records. Using a stolen password, hackers were able to break into a database which contained the personal information of former and current clients, as well as employees.

Related stories:
- Security: Who’s in charge during a cyberattack? Pentagon doesn’t know
- Security: iPhone 6S, 6S Plus vulnerable to new lock screen bypass flaw
- Security: Microsoft catches severe account

Tweet along: #Sec360 @pjktech @cohesivenet
Ashley Madison parent CEO quits after huge infidelity data hack

Toronto | By Alastair Sharp

The chief executive of infidelity website Ashley Madison’s parent company Avid Life Media has left, just over a week after hackers leaked data about millions of its clients in a massive cyber assault.

Avid Life said on Friday the departure of Noel Biderman was by “mutual agreement” and its existing senior management team would take over until a new CEO is appointed.

On Aug. 18, hackers who claimed to be unhappy with its business practices released the Ashley Madison customer data, and police probing the breach said it had sparked extortion attempts and at least two unconfirmed suicides.

The data dump contained email addresses of U.S. government officials, UK civil servants and workers at European and North American corporations, taking already deep-seated fears about Internet security and data protection to a new level.
application layer network security
application segmentation

micro-perimeter around critical apps in any environment
limit server interactions

server traffic must go through a secure app-layer switch
control network flow

traffic only flows in permitted directions, from permitted locations

Tweet along: #Sec360
@pjktech @cohesivenet
security for each app
upcoming security compliance regulations
practical, compelling needs

PR.AC-5
NIST Cyber Security Framework
“Network integrity is protected, incorporating network segregation where appropriate”
practical, compelling needs

PCI DSS
Payment Card Industry Data Security Standard v3.0
“adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not"
practical, compelling needs

US DHS Guidelines
National Cyber Security Division
Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies
upcoming security compliance regulations
EU Data Protection Directive: 2018

- data processors responsible for data protection
- tougher penalties: up to €20M
- impacts every entity that holds or uses European personal data both inside and outside of EU
- controllers must meet "reasonable expectations" of data privacy = tokenised, encrypted or anonymised data
Safe Harbor/EU-US Privacy Shield: June

- original agreement between US and EU to adhere to EU laws & standards when handling EU citizen’s data
- US companies can self-certify they are storing customer data properly
- voided in October 2015, new voted expected June 2016
industry-specific guidelines

• Federal Information Security Management Act (FISMA)
• North American Electric Reliability Corp. (NERC) standards
• Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records
• Health Insurance Portability and Accountability Act (HIPAA)
• The Health Information Technology for Economic and Clinical Health Act (HITECH)
• Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule)
• H.R. 2868: The Chemical Facility Anti-Terrorism Standards Regulation
broadly applicable laws and regulations

- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley Act (GLB) Act
- Electronic Fund Transfer Act
- Regulation E (EFTA)
- Customs-Trade Partnership Against Terrorism (C-TPAT)
- Free and Secure Trade Program (FAST)
- Children's Online Privacy Protection Act (COPPA)
- Fair and Accurate Credit Transaction Act (FACTA)
- Federal Rules of Civil Procedure (FRCP)
security takeaways

most standards say:

• encrypt sensitive data in motion and at rest whenever it is “reasonable and appropriate”

• “reasonable expectation” of companies to provide data security
here’s to a more secure 2016
segment and isolate apps
enforce traffic policies with firewalls
detect malicious traffic with NIDS
limit intra-app network traffic with WAF
create logical subnets

Define smaller subnets within an app network range along with firewall rules

Example app network Subnet - 172.31.1.0/26
monitor traffic with app-layer switches
build layers of control and access

Key security elements must be controlled by the customer, but separate from the provider.

- **Provider Owned/Provider Controlled**
- **Provider Owned/User Controlled**
- **VNS3 - User Owned/User Controlled**
- **User Owned/User Controlled**
use encrypted overlay networks

- use unique X.509 credentials for each Overlay IP address
- create a secure TLS VPN tunnel between networks
- encrypt all data in motion end-to-end
Conclusions

• data center security does not work for cloud security
• everyone is liable for weak security - including your customers
• applications need security via network virtualization
• compliance regulations emphasize network segmentation, app security and isolation
• app layer switches and network controls can make for a more secure 2016
Q&A

Stay in touch:
@pjktech
@cohesivenet

contactme@cohesive.net