Real Cloud Breach Examples from the Checkpoint Incident Response Team - 2017 Incidents:

**Story #1 - How much is my cloud bill?**

- Major Telco corporate hosted advertisement campaign on a public cloud (AWS)
- Stood up web servers globally for campaign
- Configured auto scaling to ensure the infrastructure could grow
- Simple web architecture which was copied from corporate prod (via replicating the existing AMI)
- Deployed basic available cloud controls
- Attacker found web admin vulnerability (Tomcat) and placed bit coining and DDoS malware on web server
- Infrastructure started to auto scale.....And boy did it.... Over $500K
- Read more: https://research.checkpoint.com/hey-you-get-off-of-my-cloud/

**Story #2 - Your holding my power company for ransom?**

- Customer called Incident Response Hotline and said they had a number of servers displaying a ransomware note
- Apparently the attacker had identified an open RDP server and performed brute force login attack
- Password was....unfortunately (but not uncommonly weak)...“letmein123”
- Server was a VM on a large ESX environment
- Attacker brute forces domain admin
- Attacker moved laterally and infected 50+ hosts including primary billing system
Story #3 - Who’s moving laterally in my cloud

- Customer deployed in a public cloud web hosting infrastructure
- Application developer required an SQL connection from cloud provider to backend database hosted within corporate environment
- Request a firewall port be opened for MySQL
- Corporate only deployed simple firewall and load balancer in cloud
- **Attacker found an SQL injection attack** in app and obtained shell
- Moved laterally from cloud to corporate environment

Story #4 - My cloud is attacking my other cloud, does that mean there is a storm coming

- Customers moved over to O365
- Customer deploys ADFS and AD to cloud (AWS)
- Loves the cloud so they move everything to cloud. No more infrastructure in the office....
- Deployed web servers into another cloud, because it’s cheaper, and you know two is better than one
- Ties authentication to ADFS....Man is this easy.....
- Attacker starts to **brute force login attack** on web server
- Attacker has all user emails and locks them all out in 30 mins
- Now what??????
Close to home SaaS breach:
https://www.theregister.co.uk/2016/08/16/brisbane_councillors_lose_500k_to_scammers/

For more information or if you’d like a demonstration of IPSe’s capabilities please contact your IPSec account manager.

1300 890 902

enquiry@ipsec.com.au