The Cloud Is Just Someone Else's Computer, But It's Still Your Problem

Andoni Alonso
Bsides Málaga ~ 2025

unicrons.cloud

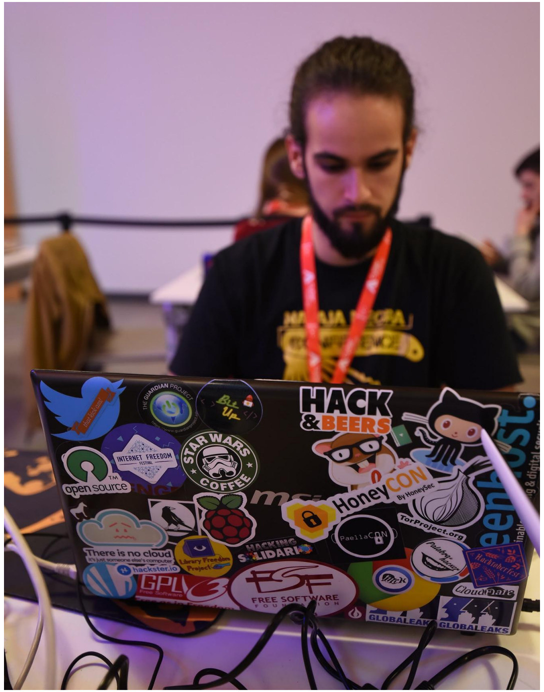
```
$ aws sts get-caller-identity
```

Andoni Alonso Fernández 🖖

- Cloud Security Engineer @ Prowler
  - Prev: SRE @ Flywire, Sysadmin...
- Writing at unicrons.cloud
- AWS User Group Leader Valencia

  & Security Community Builder
- Padel 🏓 and Geoguessr 🌍

Me last year...



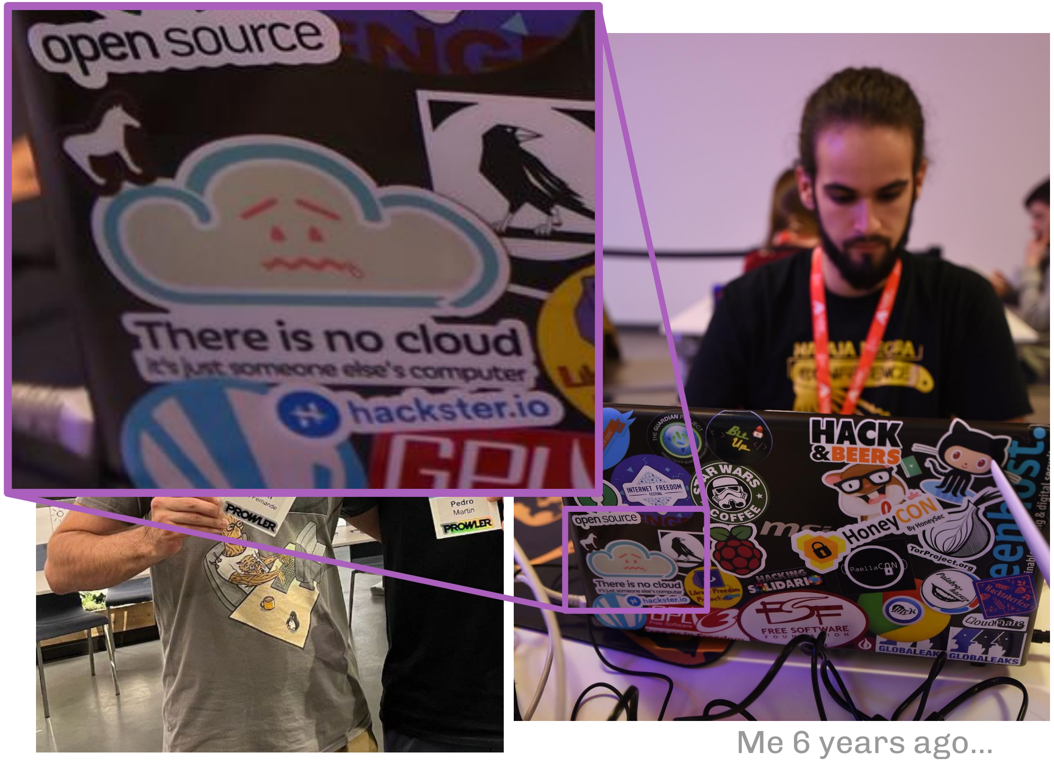
Me 6 years ago...

andoniaf.bsky.social   in andoniaf   X @andoni013

$ aws sts get-caller-identity

Andoni Alonso Fernández 🖖

- Cloud Security Engineer @ Prowler
  - Prev: SRE @ Flywire, Sysadmin...
- Writing at unicrons.cloud
- AWS Valencia User Group Leader
- Padel 🏓 and Geoguessr 🌍

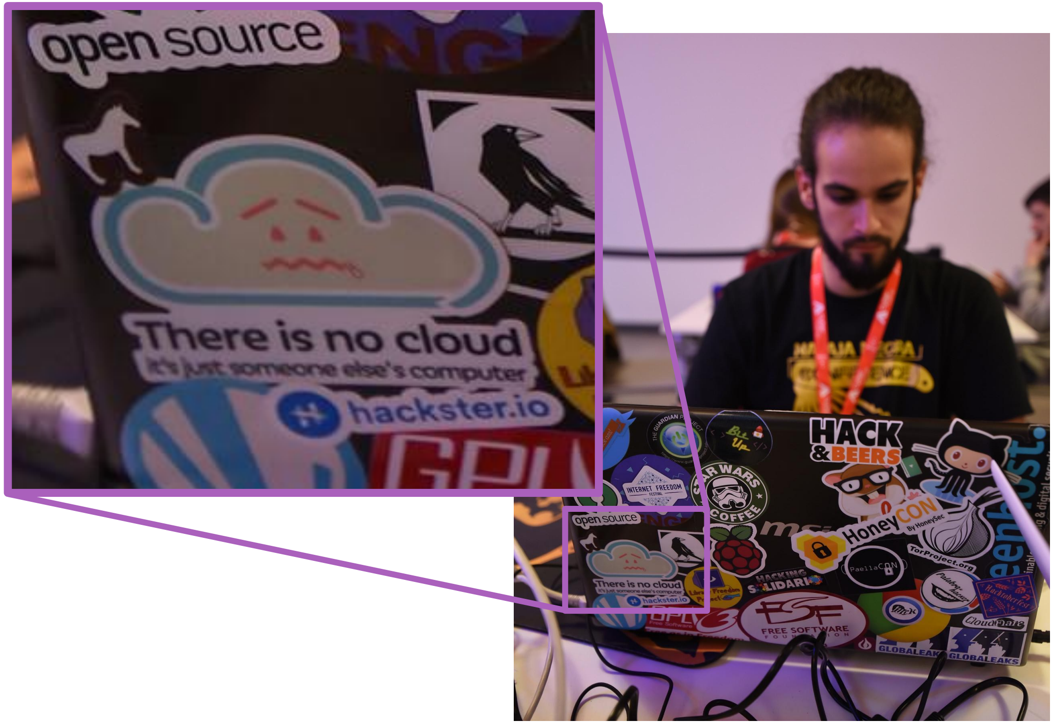


Me 6 years ago...

🦋 andoniaf.unicrons.cloud in andoniaf 𝕏 @andoni013

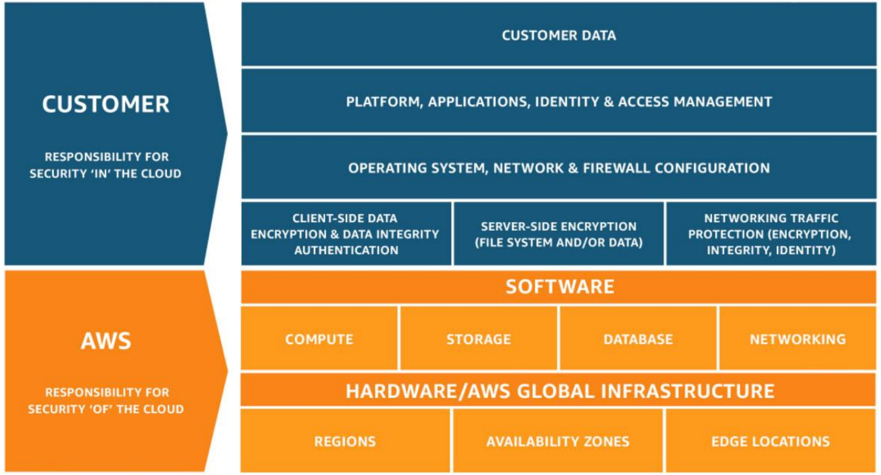
There is no cloud, it's just some else's computer

- What does that means for us?



There is no cloud, it's just some else's computer

- What does that means for us?
  - ○ Security “**of**” the cloud
  - ○ Security “**in**” the cloud



CUSTOMER

RESPONSIBILITY FOR SECURITY ‘IN’ THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY ‘OF’ THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

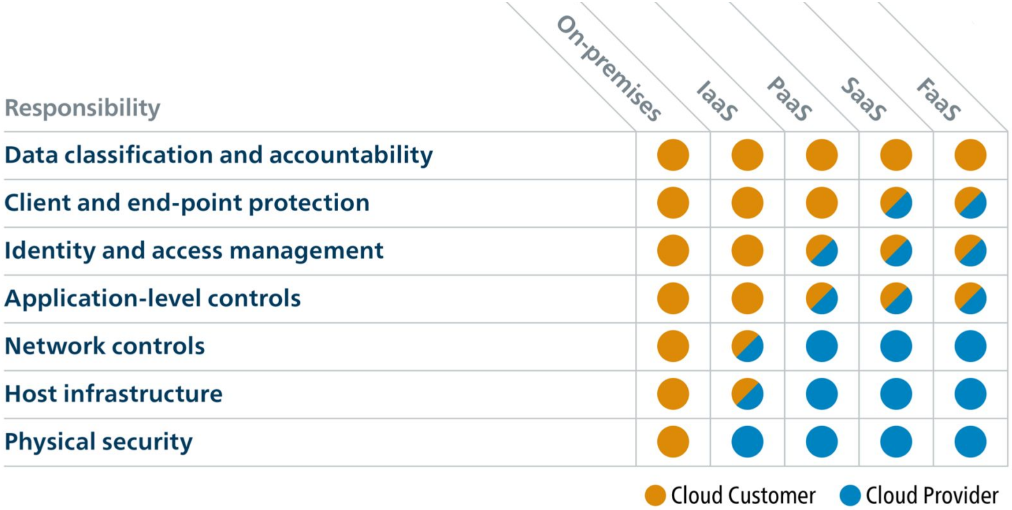
HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

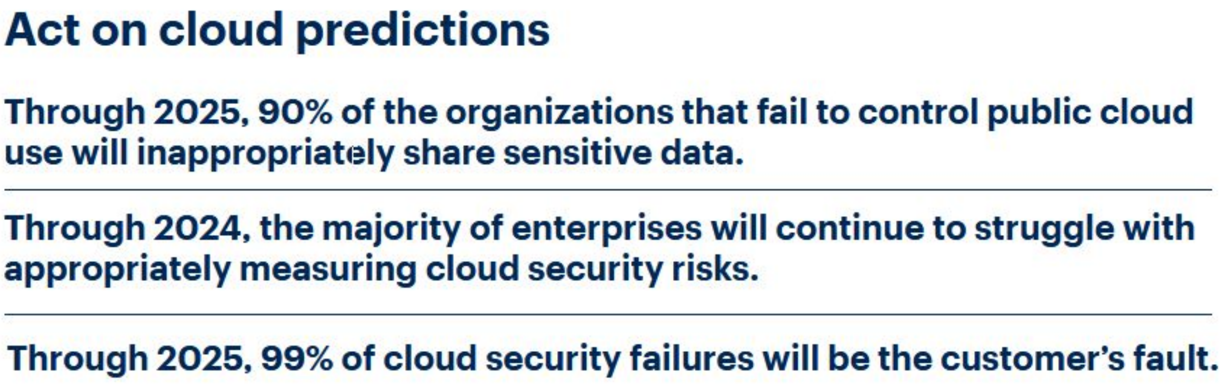
From https://aws.amazon.com/es/compliance/shared-responsibility-model/



Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS
Data classification and accountability	🟠	🟠	🟠	🟠	🟠
Client and end-point protection	🟠	🟠	🟠	🟠🔵	🟠🔵
Identity and access management	🟠	🟠	🟠🔵	🟠🔵	🟠🔵
Application-level controls	🟠	🟠	🟠🔵	🟠🔵	🟠🔵
Network controls	🟠	🟠🔵	🔵	🔵	🔵
Host infrastructure	🟠	🟠🔵	🔵	🔵	🔵
Physical security	🟠	🔵	🔵	🔵	🔵

🟠 Cloud Customer 🔵 Cloud Provider

From https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know



Act on cloud predictions

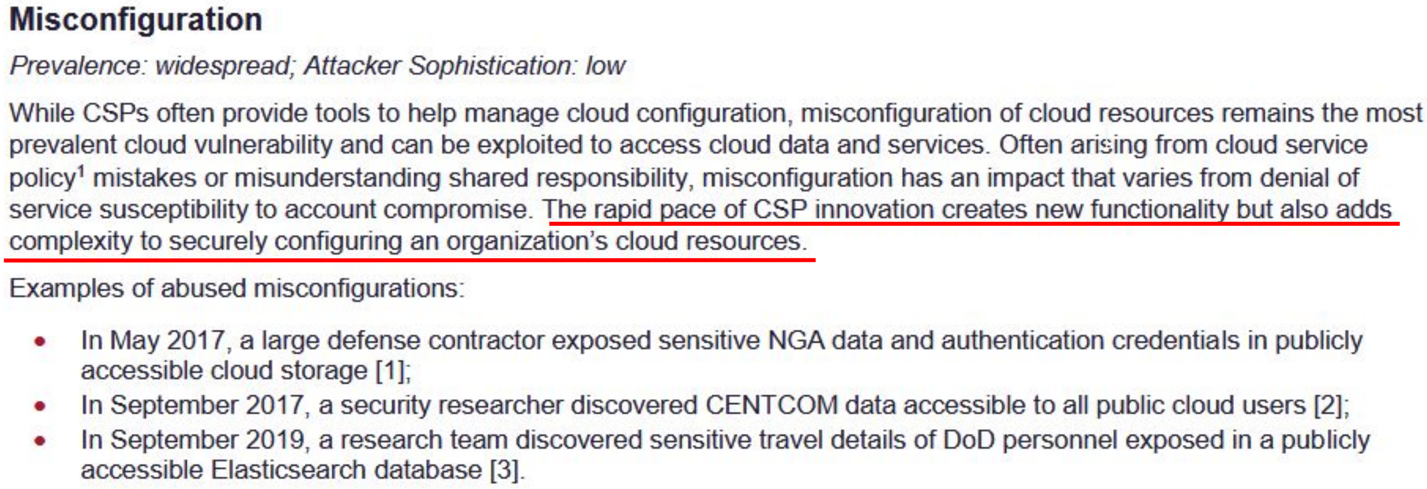
Through 2025, 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data.

Through 2024, the majority of enterprises will continue to struggle with appropriately measuring cloud security risks.

Through 2025, 99% of cloud security failures will be the customer's fault.

https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF



Misconfiguration

Prevalence: widespread; Attacker Sophistication: low

While CSPs often provide tools to help manage cloud configuration, misconfiguration of cloud resources remains the most prevalent cloud vulnerability and can be exploited to access cloud data and services. Often arising from cloud service policy[1] mistakes or misunderstanding shared responsibility, misconfiguration has an impact that varies from denial of service susceptibility to account compromise. The rapid pace of CSP innovation creates new functionality but also adds complexity to securely configuring an organization's cloud resources.

Examples of abused misconfigurations:

- In May 2017, a large defense contractor exposed sensitive NGA data and authentication credentials in publicly accessible cloud storage [1];
- In September 2017, a security researcher discovered CENTCOM data accessible to all public cloud users [2];
- In September 2019, a research team discovered sensitive travel details of DoD personnel exposed in a publicly accessible Elasticsearch database [3].

MYTHBUSTERS

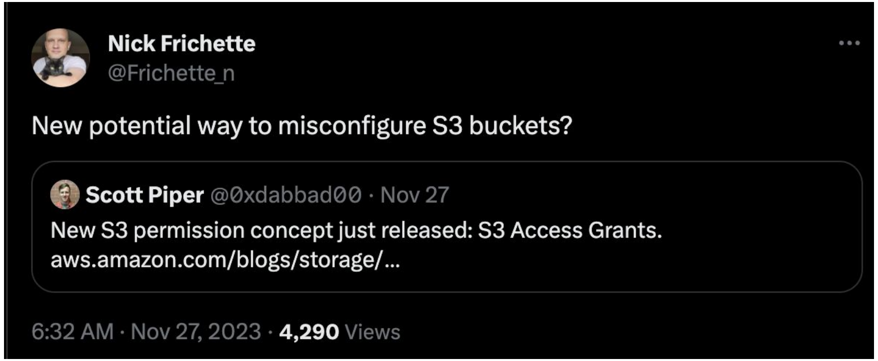
The "Set It and Forget It" Myth

Misconception: "We moved to the cloud, so security is handled for us."

The "Set It and Forget It" Myth

Misconception: "We moved to the cloud, so security is handled for us."

Reality: Cloud security is an ongoing process, not a one-time setup.



Nick Frichette
@Frichette_n

New potential way to misconfigure S3 buckets?

> **Scott Piper** @0xdabbad00 · Nov 27
> New S3 permission concept just released: S3 Access Grants.
> aws.amazon.com/blogs/storage/...

6:32 AM · Nov 27, 2023 · **4,290** Views

The "Cloud = More Secure Than On-Prem" Myth

Misconception: "Cloud providers are huge companies with advanced security, so it’s automatically safer than my data center."

The "Cloud = More Secure Than On-P

Misconception: "Cloud providers are huge companies with advanced security, so it’s automatically safer than my data center."

Reality: The cloud is only as secure as your configurations.

The "We Have a Firewall, We're Safe" Myth

Misconception: "If I set up a firewall (or Security Group), my cloud environment is secure."

The "We Have a Firewall, We’re Safe" M

MYTH BUSTED

Misconception: "If I set up a firewall (or Security Group), my cloud environment is secure."

Reality: Firewalls don’t stop over-permissioned IAM roles, weak API keys, or unpatched applications.

But, what is a misconfiguration?

Crowdstrike: “Security misconfiguration is any error or vulnerability present in the configuration of code that allows attackers access to sensitive data.”

expertinsights: “Misconfiguration, or human error, is when computing assets (in this case, cloud assets) are set up incorrectly. This leaves them vulnerable to malicious activity, and can mean that security incidents or breaches aren’t picked up as quickly.”

Upguard: “Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption.”

But, what is a misconfiguration?

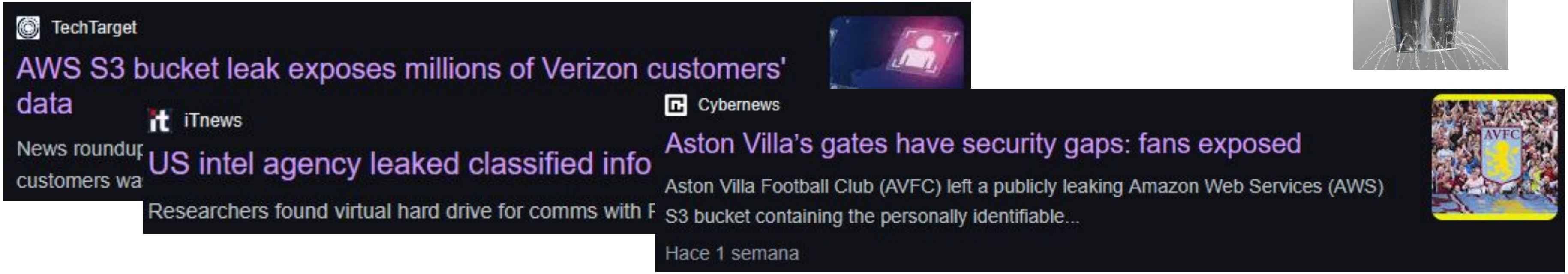
Crowdstrike: **“Security misconfiguration is any error or vulnerability present in the configuration** ~~of code~~ **that allows** ~~attackers access to sensitive data~~ **to cause damage .”**

expertinsights: “Misconfiguration, or human error, is when computing assets (in this case, cloud assets) are set up incorrectly. This leaves them vulnerable to malicious activity, and can mean that security incidents or breaches aren’t picked up as quickly.”

Upguard: “Cloud misconfiguration refers to any glitches, gaps, or errors that could expose your environment to risk during cloud adoption.”

Welcome,
to the real
world

Real World Examples: S3 leaks



TechTarget

AWS S3 bucket leak exposes millions of Verizon customers' data

News roundup

customers wa

iTnews

US intel agency leaked classified info

Researchers found virtual hard drive for comms with F

Cybernews

Aston Villa's gates have security gaps: fans exposed

Aston Villa Football Club (AVFC) left a publicly leaking Amazon Web Services (AWS) S3 bucket containing the personally identifiable...

Hace 1 semana

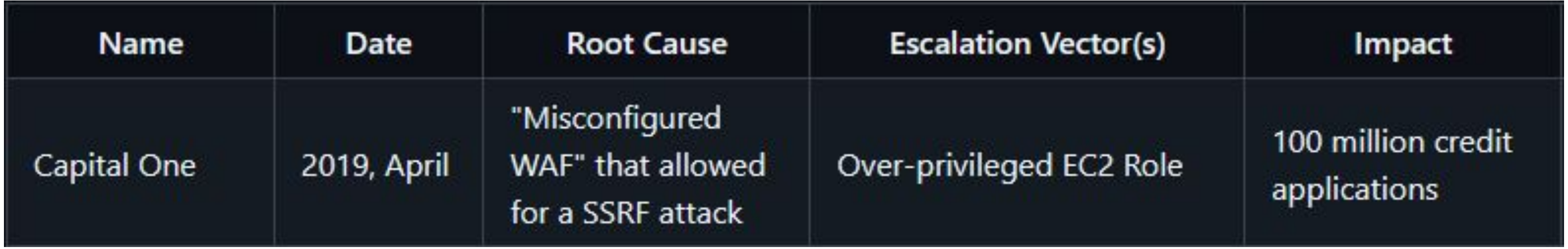
What Happened?

- Many organizations left Amazon **S3 buckets publicly accessible**, exposing **sensitive data** like customer PII, internal passwords, and confidential documents..

Lesson:

- **Check and enforce bucket permissions—**public S3 buckets should be the exception, not the default.
  - Use **CSPM** tools (Cloud Security Posture Management) to detect misconfigurations.
- **Encrypt** sensitive data at rest and in transit.

Real World Examples: Capital One



Name	Date	Root Cause	Escalation Vector(s)	Impact
Capital One	2019, April	"Misconfigured WAF" that allowed for a SSRF attack	Over-privileged EC2 Role	100 million credit applications

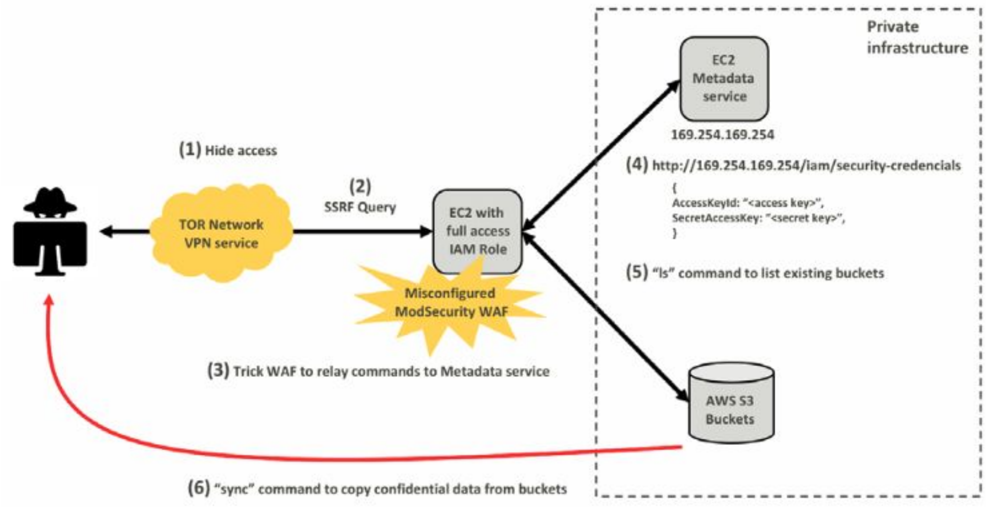
https://cloudsecurityalliance.org/blog/2019/08/09/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach
https://www.capitalone.com/digital/facts2019/

What Happened?

- An outside individual gained access through a **misconfigured WAF** and a SSRF vulnerability.
- Then used the **instance IAM role** to **steal** data from Capital One S3 buckets.
- **100 million+ customer records** were exposed, including Social Security numbers and credit applications.

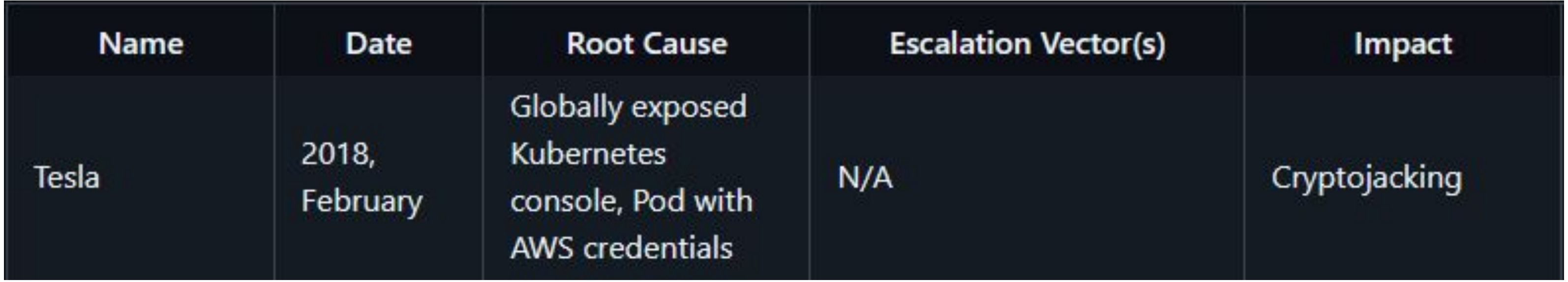
Lesson:

- **Least privilege IAM policies** are critical, don't allow unnecessary permissions.
- Always **monitor** and **audit** IAM roles and access logs.


Private infrastructure
EC2 Metadata service
169.254.169.254
(1) Hide access
(2) SSRF Query
TOR Network VPN service
EC2 with full access IAM Role
Misconfigured ModSecurity WAF
(4) http://169.254.169.254/iam/security-credencials
{
AccessKeyId: "<access key>",
SecretAccessKey: "<secret key>",
}
(5) "ls" command to list existing buckets
(3) Trick WAF to relay commands to Metadata service
AWS S3 Buckets
(6) "sync" command to copy confidential data from buckets

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3570138

Real World Examples: Tesla



Name	Date	Root Cause	Escalation Vector(s)	Impact
Tesla	2018, February	Globally exposed Kubernetes console, Pod with AWS credentials	N/A	Cryptojacking

https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/

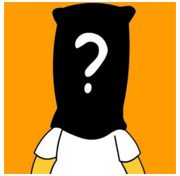
What Happened?

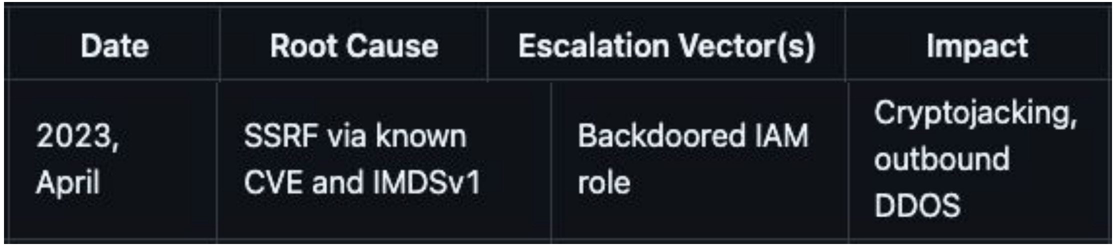
- Attackers found Tesla’s **Kubernetes dashboard exposed to the internet without authentication**.
- They deployed **cryptocurrency miners** inside Tesla’s cloud environment, stealing compute resources.

Lesson:

- **Never expose internal dashboards/APIs to the public.**
- Use IAM roles, **MFA**, and firewalls to restrict access.
- **Monitor cloud resource usage**— unexpected spikes may indicate hijacking.

Real World Examples: ??





Date	Root Cause	Escalation Vector(s)	Impact
2023, April	SSRF via known CVE and IMDSv1	Backdoored IAM role	Cryptojacking, outbound DDOS

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/unit42-cloud-threat-report-volume7.pdf

What Happened?

- Internal web server was accidentally made public due to a **misconfigured security group** setting during a migration process.
- Server was vulnerable to Server Side Request Forgery (**SSRF**) allowing attackers to send HTTP requests to hosts behind the firewall.
- Usage of outdated **IMDSv1** allowed the threat actor to exfiltrate temporary credentials associated with the VM instance.
- Cryptomining and DDoS attacks using their infrastructure.

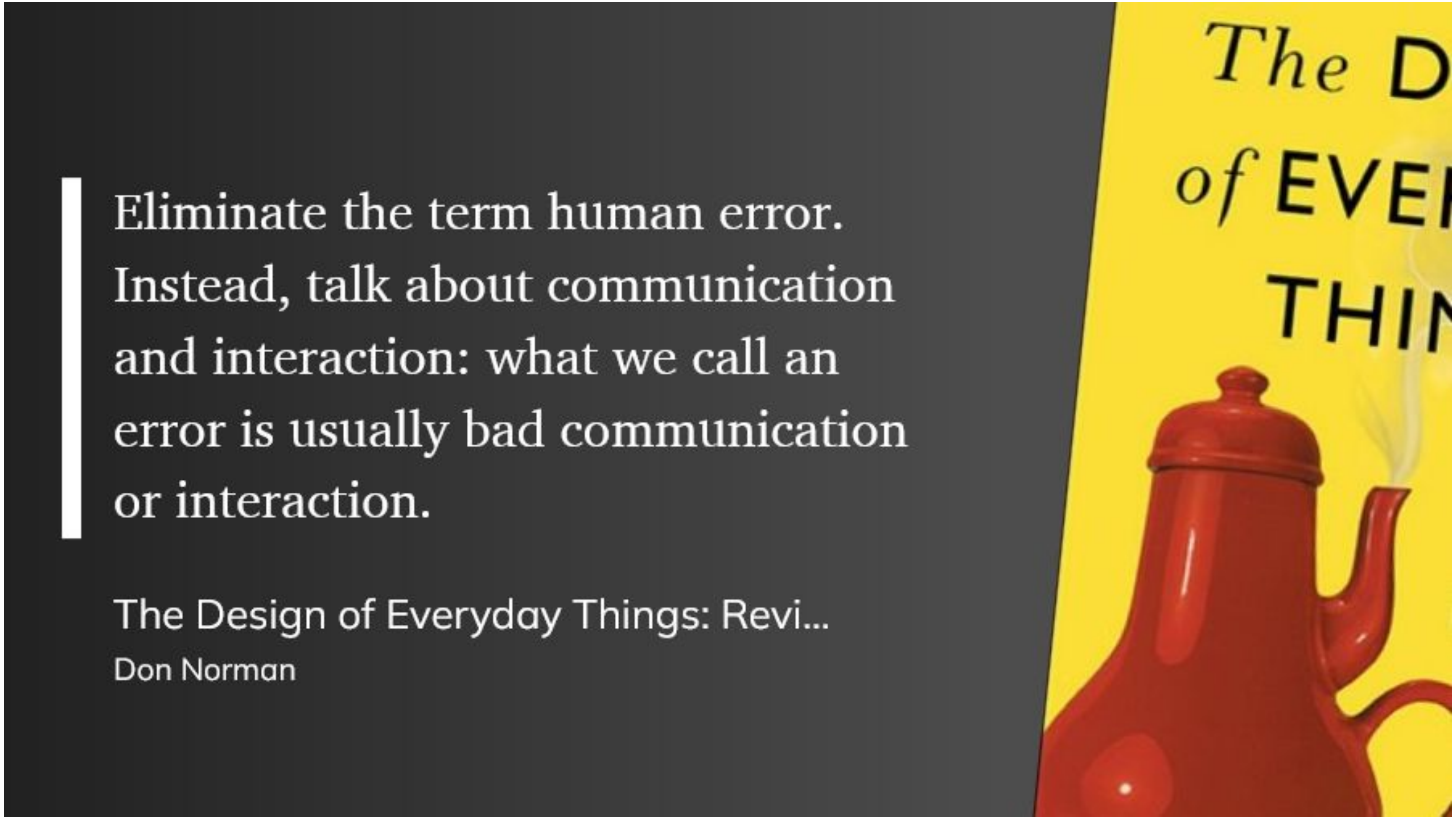
Lesson:

- Same as previous slides. 😅

Yes, the cloud is complex…

but that doesn’t mean it’s bad.

The Social Construction of Human Error



> Eliminate the term human error. Instead, talk about communication and interaction: what we call an error is usually bad communication or interaction.

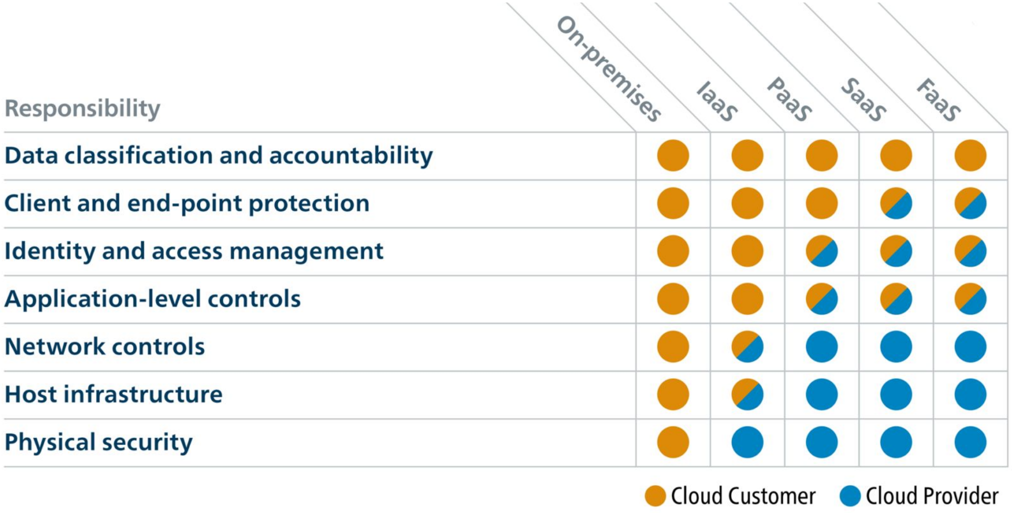
The Design of Everyday Things: Revi...

Don Norman

The D
of EVE
THI

Solutions and Best Practices

1. **Follow the Shared Responsibility Model**
   - Understand what the cloud provider secures vs. what you must secure.
   - Don’t assume default configurations are secure.



Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS
Data classification and accountability	🟠	🟠	🟠	🟠	🟠
Client and end-point protection	🟠	🟠	🟠	🟠/🔵	🟠/🔵
Identity and access management	🟠	🟠	🟠/🔵	🟠/🔵	🟠/🔵
Application-level controls	🟠	🟠	🟠/🔵	🟠/🔵	🟠/🔵
Network controls	🟠	🟠/🔵	🔵	🔵	🔵
Host infrastructure	🟠	🟠/🔵	🔵	🔵	🔵
Physical security	🟠	🔵	🔵	🔵	🔵

🟠 Cloud Customer 🔵 Cloud Provider

From https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know

Solutions and Best Practices

2. **Principle Of Least Privilege, Always**
   - Only give users/services the permissions they absolutely need.
   - Enable Multi-Factor Authentication (MFA).
   - Use roles instead of long-lived access keys.

Solutions and Best Practices

3. **Monitor & Audit Continuously**
   - Proactive monitoring helps detect misconfigurations early.
   - Enable CloudTrail, GuardDuty, and Security Hub (AWS) or equivalent tools in Azure/GCP.
   - Use Cloud Security Posture Management (CSPM) tools like Prowler

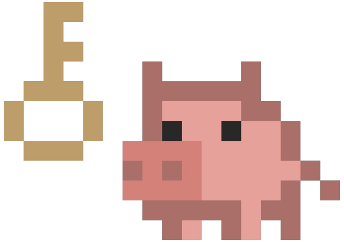
AWS Security Hub

Amazon GuardDuty

AWS CloudTrail

Solutions and Best Practices

4. **Automate Security & Compliance (Shift-Left Security)**
   - Security shouldn’t be an afterthought
   - Use Infrastructure as Code (IaC) security scanners like [checkov](), [trivy]() or [trufflehog]() to catch misconfigurations early.
   - Automate security policy enforcement using CI/CD pipeline checks.
   - Use automated compliance checks to ensure cloud configurations meet industry standards (NIST, CIS, SOC 2).



Solutions and Best Practices

5. **Stay Updated on Cloud Security Best Practices**
    - Cloud security is constantly evolving, so stay ahead of threats.
    - Follow AWS Well-Architected Framework, Azure Security Center, or Google Cloud Security Best Practices.
    - Subscribe to newsletters, security blogs, follow **unicrons.cloud** SPAM

AWS SECURITY DIGEST

CLOUDSECLIST
by Marco Lancini

Solutions and Best Practices

6. **Test Your Security**
    - Regular security testing is key to finding weaknesses before attackers do.
    - Conduct cloud penetration testing & red team exercises.
        - Use attack simulation tools (like Pacu for AWS) to test security controls.
    - Participate in bug bounty programs to find vulnerabilities.

Final thoughts

- **Cloud security** isn't a set-it-and-forget-it task—it's an **ongoing process**.
- **Educate** you and yours teams on cloud security to avoid "human errors".
- Go choose the **CSPM** you think it will fit best for your environment and start auditing your cloud.

Because remember:

It may be just someone else's computer...

...but it's still your problem!

Thanks!

Any question?

andoniaf

andoniaf.unicrons.cloud

unicrons.cloud

@andoni013

@unicrons_cloud

References and extra info:

- How to 10X Your Cloud Security (Without the Series D) ~ Rami McCarthy @ fwd:cloudsec EU 24
  - github.com/ramimac
- Newsletters:
  - AWS Security Digest
  - CloudSec List
  - tldr sec
- IAM policy mishaps: Intro to IAM
- github.com/4ndersonLin/awesome-cloud-security
- opencloudsecurity.org/blog (CFP Open!)

It may be just someone else's computer...

...but it's still your problem!