The COVID-19 Pandemic And Its Influence On Cloud Cyber Security

FAST-CSP: Finding a Solution to Cloud Security Problems

Andreas Aßmuth

Technical University of Applied Sciences
OTH Amberg-Weiden, Amberg, Germany

April 24, 2021 to April 28, 2022

About me

Professor of Computer Networks and Mathematics

Dean of Studies (Department of Electrical Engineering, Media and Computer Science)

Teaching:

- Mathematics, Computer Networks, Cryptography, Coding Theory, Information Security

Research:

- Applied Cryptography, Information Security, Ethical Hacking

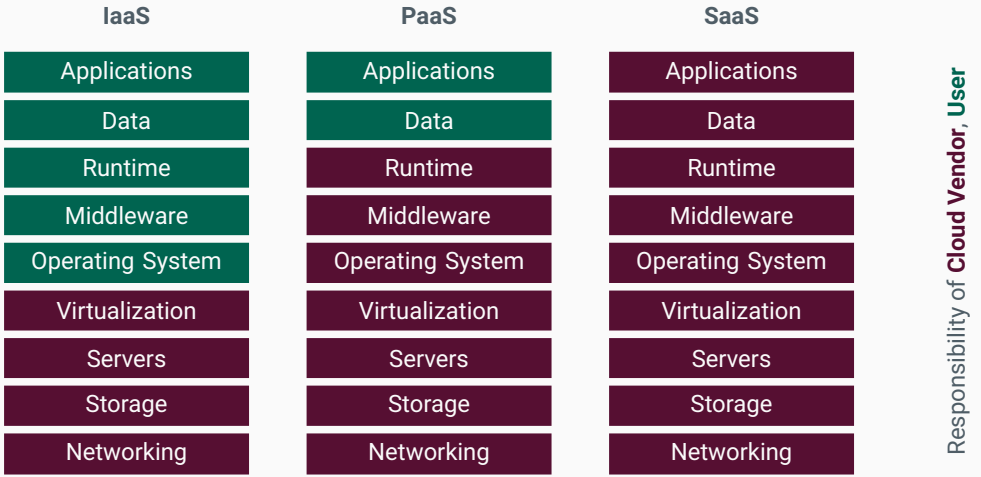
IARIA Fellow

Outline

1. Cloud Security Challenges before the Pandemic
2. Pandemic-related Attacks
3. Traditional Attacks
4. Conclusion

Cloud Cyber Security A rather complex issue...

Cloud Security Responsibility Model



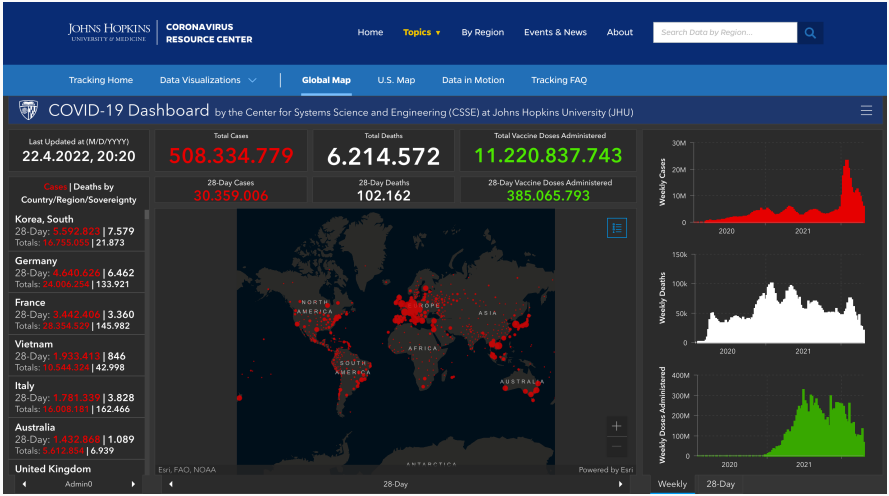
Source: National Security Agency, *Cybersecurity Information – Cloud Security Basics.*
URL: `https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-cloud-security-basics.pdf`, 2018-08-29.

Cloud Cyber Challenges 2019

Rank	Security challenge	Score
1	Malware infection (Cloud infrastructure)	8.1
2	Unauthorised access	7.7
3	Man in the middle attacks	7.5
4	DDoS attacks	7.2
5	Data loss	6.6
6	Rerouting	5.7

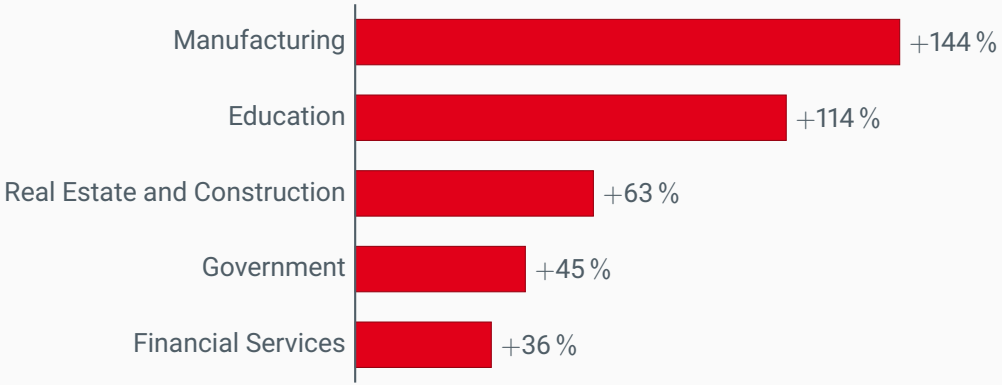
Source: Fabian Süß, Marco Freimuth, Andreas Aßmuth, George R S Weir, and Bob Duncan, *Cloud Security and Security Challenges Revisited*, CLOUD COMPUTING 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization, Venice, Italy, 5 to 9 May 2019, Proceedings, pp. 61-66, 2019.

COVID-19 Pandemic



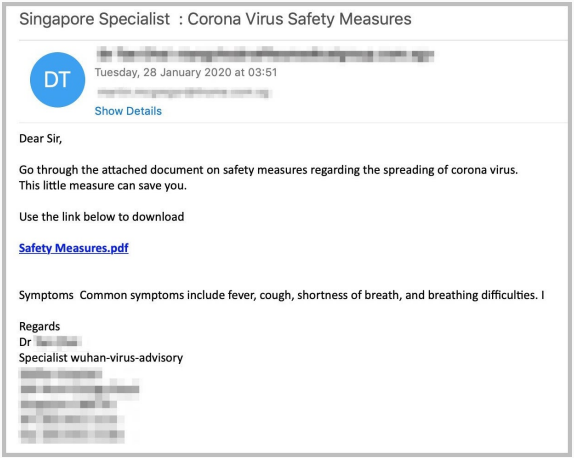
Screenshot taken from `https://coronavirus.jhu.edu/map.html`, 2022-04-22.

Overall Cloud Service Usage Increases January to April 2020



Data Source: McAfee, *Cloud Adoption and Risk Report, Work from Home Edition.* p. 3, May 2020.

COVID-19 Phishing Scams I



Singapore Specialist : Corona Virus Safety Measures

DT

Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

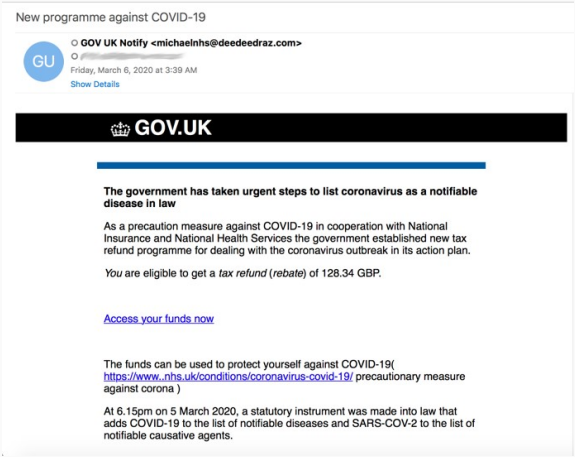
Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr
Specialist wuhan-virus-advisory

Image Source: Lily Hay Newman, *Watch Out for Coronavirus Phishing Scams*. wired.com, 2020-01-31, https://www.wired.com/story/coronavirus-phishing-scams/.

COVID-19 Phishing Scams II



New programme against COVID-19

GU

GOV UK Notify <michaelnhs@deedeedraz.com>

Friday, March 6, 2020 at 3:39 AM

Show Details

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

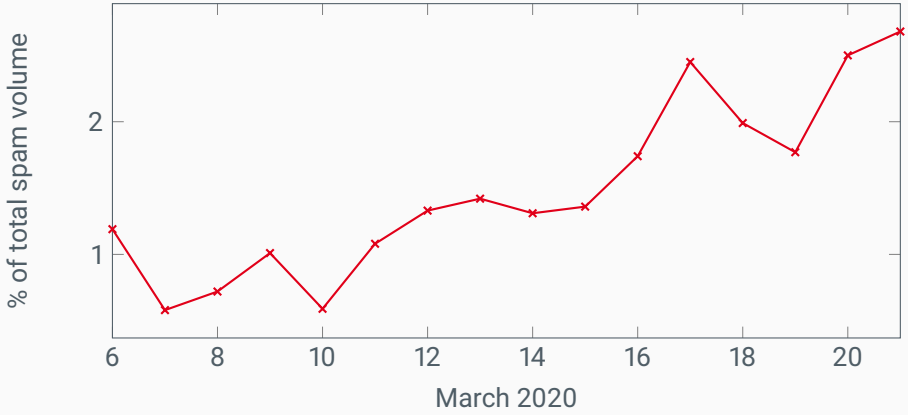
Access your funds now

The funds can be used to protect yourself against COVID-19(https://www..nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

Image Source: Adrien Gendre, *Hacker nutzen die Coronavirus-Pandemie für die aktuellsten, auf Ereignis basierenden E-Mail-Angriffe*. VadeSecure, 2020-04-02, `https://www.vadesecure.com/de/hacker-nutzen-die-coronavirus-pandemie-fur-die-aktuellsten-auf-ereignis-basierenden-e-mail-angriffe/`.

COVID-19 Email Scams III



Data Source: Sophos 2021 Threat Report, p. 20, 2020.

COVID-19 Themed Android Malware

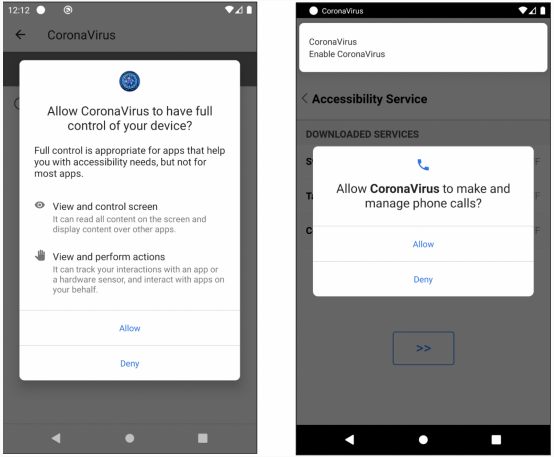


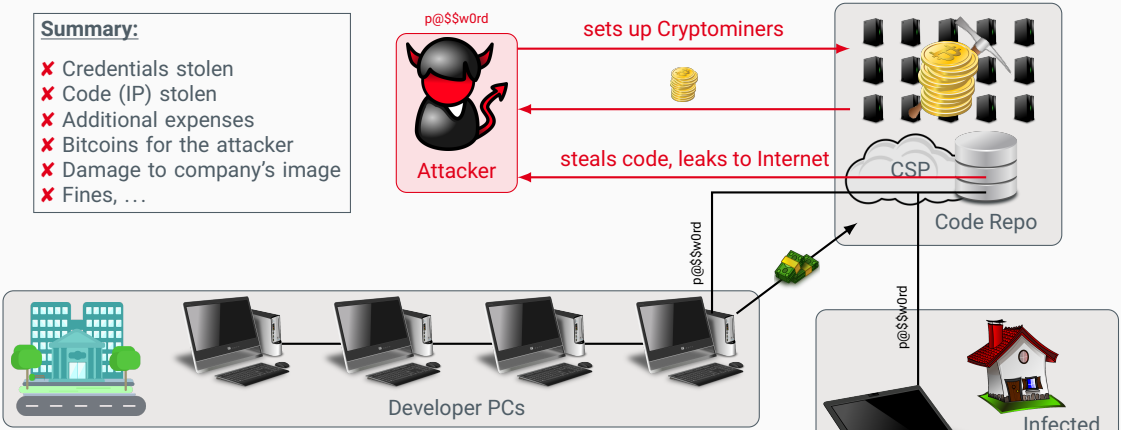
Image Source: Avira Protection Labs, *Malware Threat Report: Q2 2020 Statistics and Trends*. avira.com, 2020-09-29, https://www.avira.com/en/blog/malware-threat-report-q2-2020-statistics-and-trends.

Attacks Against Hospitals During COVID-19 Pandemic

Fictional Cloud Security Breach Scenario

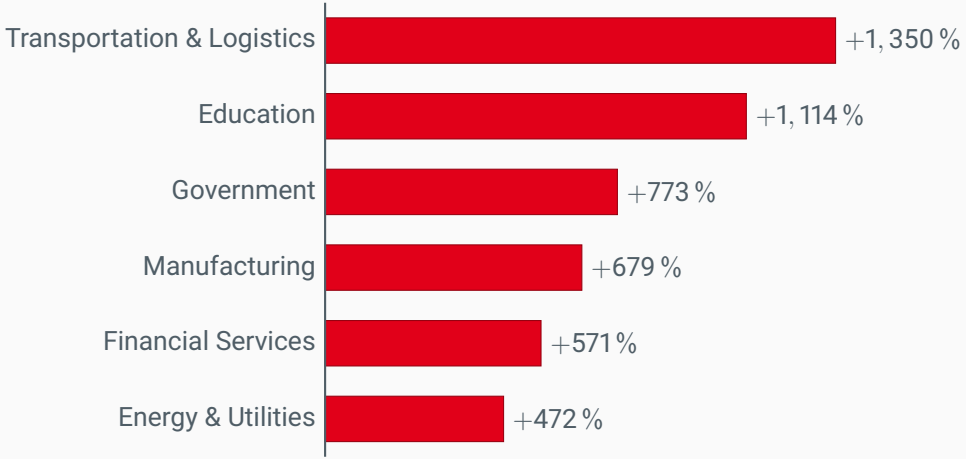
Summary:

- ✘ Credentials stolen
- ✘ Code (IP) stolen
- ✘ Additional expenses
- ✘ Bitcoins for the attacker
- ✘ Damage to company's image
- ✘ Fines, …



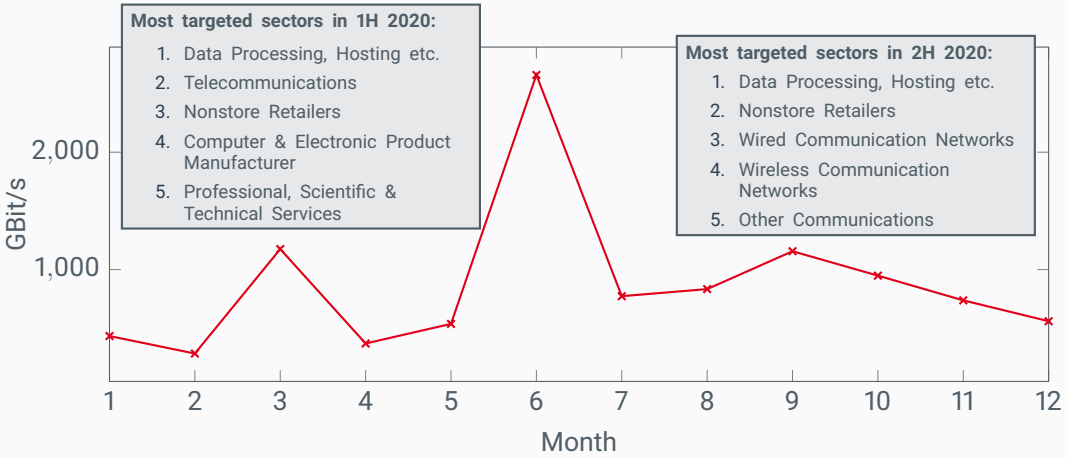
Source: Sophos 2020 Threat Report, p. 21, 2019.
Image Sources: Pixabay, https://www.pixabay.com, and OpenClipart, https://openclipart.org, CC0

Increase in Cloud Threat Events by Industry



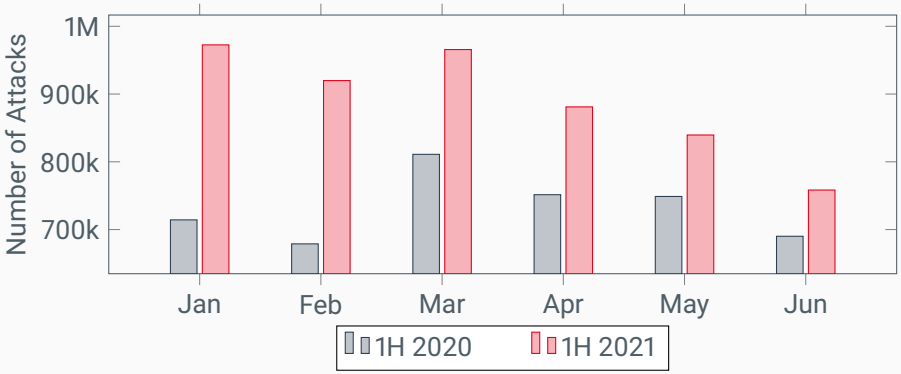
Data Source: McAfee, *Cloud Adoption and Risk Report, Work from Home Edition.* p. 6, May 2020.

COVID-19 Pandemic and DDoS Attacks Germany



Data Sources: NETSCOUT Threat Intelligence Report, *The DDoS Chronicles, Key Metrics from the 1H 2020.* 2020.
NETSCOUT Threat Intelligence Report, *The DDoS Chronicles, Key Metrics from the 2H 2020.* 2020.

Monthly DDoS Attack Frequency Germany



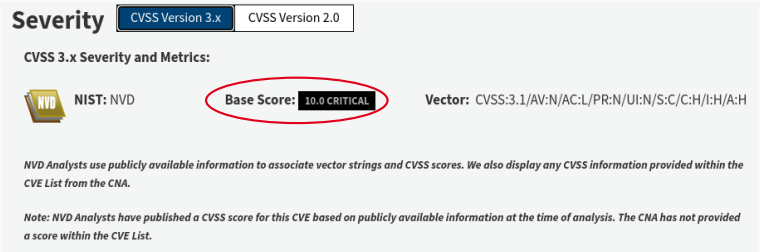
Data Source: NETSCOUT Threat Intelligence Report, Issue 7: Findings from 1H 2021, p. 7, 2021.

Log4Shell CVE-2021-44228

WIRED ‘The Internet Is on Fire’

A vulnerability in the Log4j logging framework has security teams scrambling to put in a fix.

ZDNet Log4j: How hackers are using the flaw to deliver this new 'modular' backdoor



The Problem with 3rd Party Software

76 % of companies have 3rd party roles that allow full account takeover!

82 % of companies provide 3rd party vendors highly privileged roles!

> 90 % of cloud security teams were not aware they gave high permissions to 3rd party vendors!

Source: WIZ 2022 cloud security threats, p. 6, 2022.

Data Breaches Examples

Company	Breach Scale	Date
Microsoft	250M records	January 2020
Estée Lauder	440M records	January 2020
CAM4	10B+ records	March 2020
Easyjet	9M records	May 2020
Clubillion	200M records per day	July 2020
VIP Games	23M records	January 2021
Reverb	5.6M records	April 2021
The Telegraph	10TB records	September 2021

Sources:
WIZ 2022 cloud security threats, p. 4, 2022.
Alon Schindel, *How 2021's cloud threats have matured our security strategy.* CSA Webinar, 2022-03-22.
StealthLabs, *The Biggest Data Breaches and Attacks of 2020.* URL: `https://www.stealthlabs.com/blog/the-25-biggest-data-breaches-and-attacks-of-2020/`, 2020-12-16.

Stick to the Basics! Personal Conclusion

Saltzer & Schroeder's Design Principles

- Fail-safe Defaults
- Least Privilege
- Economy of Mechanism
- Complete Mediation
- Separation of Privilege
- Open Design
- Least Common Mechanism
- Compromise Recording
- . . .

Basic Security Functions

- Identification and Authentication
- Management of Privileges
- Validation of Privileges
- Conservation of Evidence
- Reprocessing
- Ensuring functionality

Saltzer, Jerome H., and Michael D. Schroeder, *The Protection of Information in Computer Systems.* In: Proceedings of the IEEE, Vol. 63, No. 9, pp. 1278-1308, 1975.
Eckert, Claudia, *IT-Sicherheit. Konzepte, Verfahren, Protokolle.* 10. Edition, pp. 201-205, De Gruyter Oldenbourg, 2018.

Conclusion

- Pandemic caused rapid increase of cloud service usage
- Events with global impact have been used for cyber attacks before
- Cloud vendors have made a reasonable job, taken the drastic increase of users into account
- Traditional threats and security challenges must still be dealt with
- Complexity and lacking visibility of cloud environments make cloud cyber security a challenging task
- Don’t neglect the basic cyber security principles!

Prof. Dr. Andreas Aßmuth
Professor of Computer Networks and Mathematics

OTH Amberg-Weiden
Department of Electrical Engineering, Media and Computer Science

Kaiser-Wilhelm-Ring 23, 92224 Amberg, Germany
Phone: +49 9621 482 3604
Email: a.assmuth@oth-aw.de
PGP: 0xE1895723
Web: https://www.andreas-assmuth.de