Low hanging fruit DACYS TP2

Nuno Peralta
Nsp@isep.ipp.pt

isep Instituto Superior de Engenharia do Porto

O que é uma "Low hanging fruit"?

"The obvious or easy things that can be most readily done or dealt with in achieving success or making progress toward an objective"

The best way to protect data security is to get rid of all the humans.

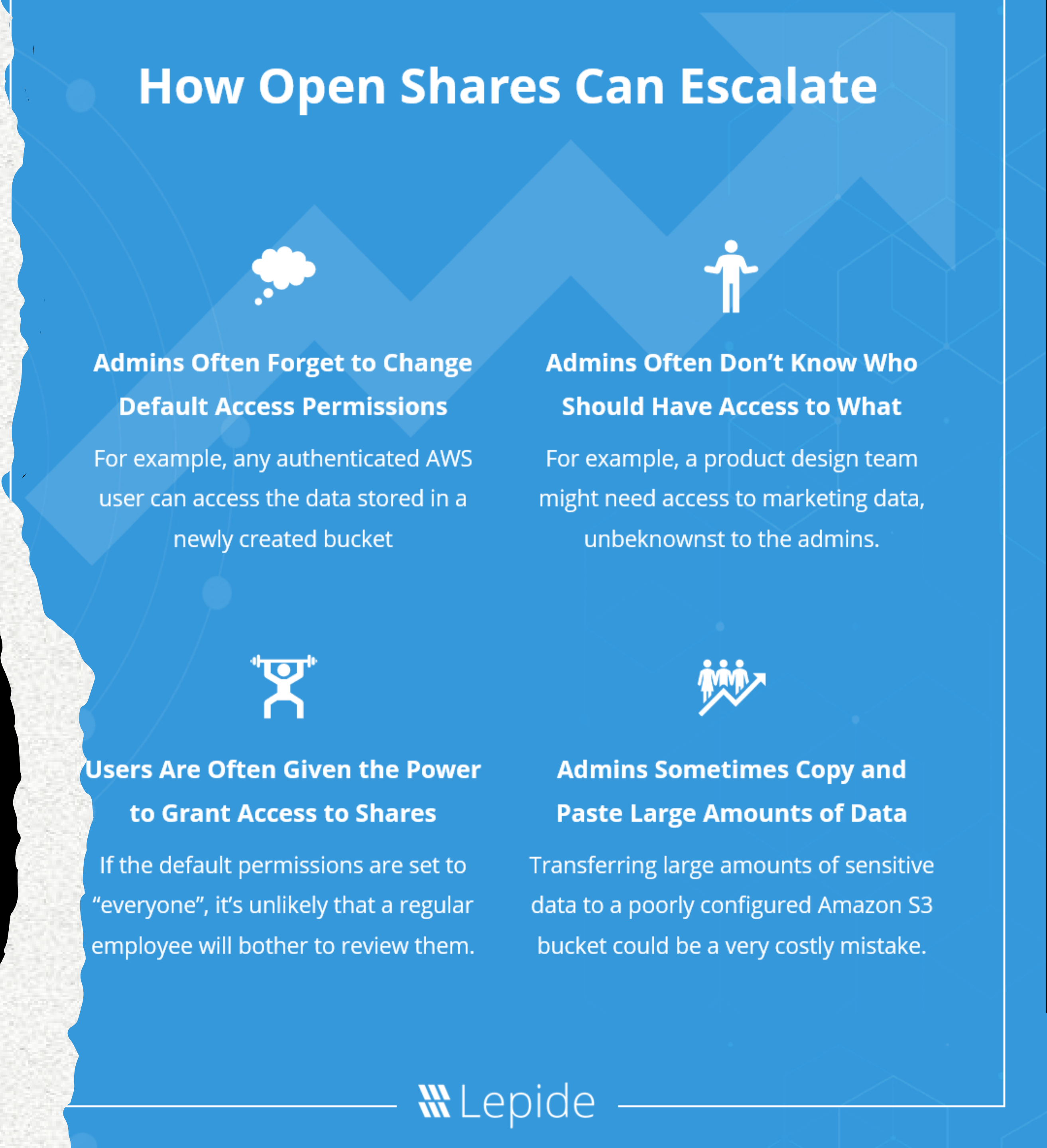
Plan B is to train them.

Vetores de ataques comuns

Credenciais fracas

Shares mal configuradas

- www.Lepid.com



How Open Shares Can Escalate

Admins Often Forget to Change Default Access Permissions

For example, any authenticated AWS user can access the data stored in a newly created bucket

Admins Often Don't Know Who Should Have Access to What

For example, a product design team might need access to marketing data, unbeknownst to the admins.

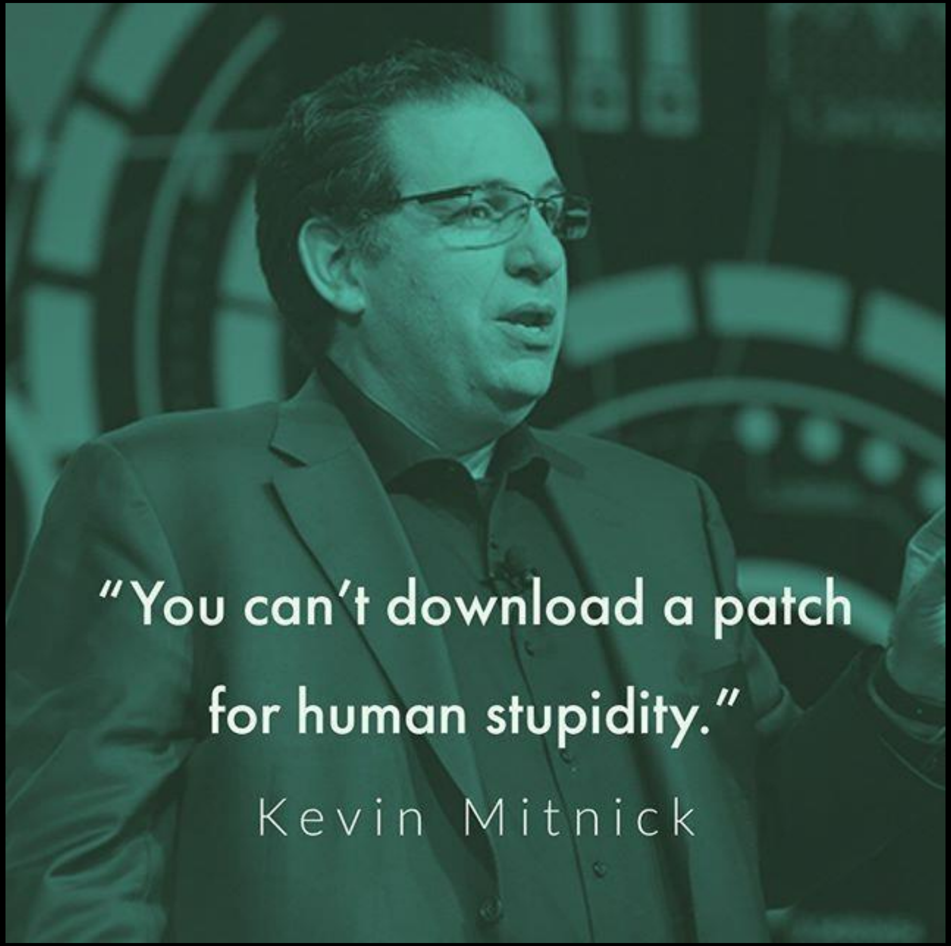
Users Are Often Given the Power to Grant Access to Shares

If the default permissions are set to "everyone", it's unlikely that a regular employee will bother to review them.

Admins Sometimes Copy and Paste Large Amounts of Data

Transferring large amounts of sensitive data to a poorly configured Amazon S3 bucket could be a very costly mistake.

Vulnerabilidades com "exploits" públicos



"You can't download a patch for human stupidity."

Kevin Mitnick

E por último...

Equivalente na vida real

Exemplo mais recente

- London Police Arrested 17-Year-Old Hacker Suspected of Uber and GTA 6 Breaches

- https://www.computerweekly.com/news/252525030/Uber-suffers-major-cyber-attack

Como tudo começou

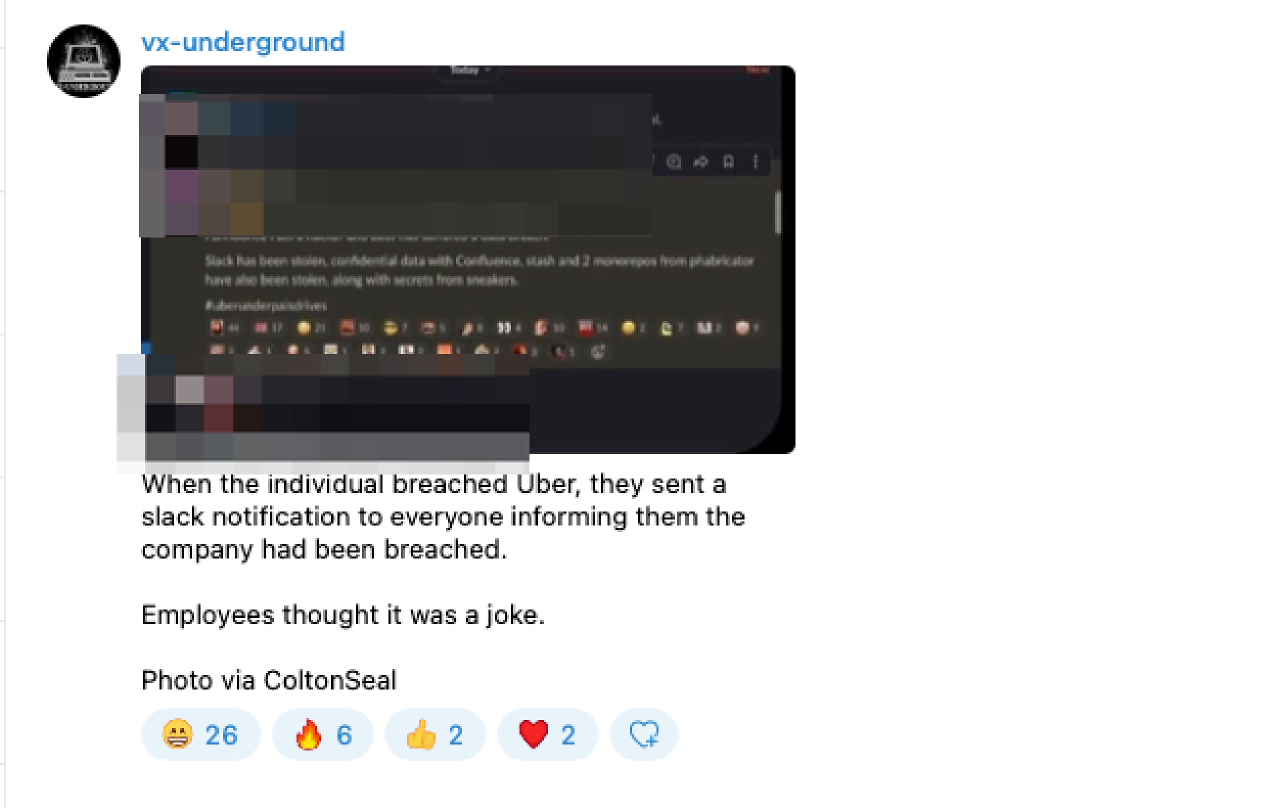
"The NYT additionally revealed that the attacker had told its reporters they had compromised Uber after successfully breaching an employee’s network access by sending them text messages posing as an internal IT admin to obtain their credentials."

O que estará depois do primeiro acesso?

"From there, they appear to have been able to establish persistence and gain access to the majority of Uber’s internal resources after scanning the company’s network and finding a PowerShell script that contained privileged credentials for an admin user of Thycotic, a provider of privileged access management (PAM) solutions. These credentials gave the attacker further access to multiple services."

Nem tudo está perdido, certo?

"Among the systems claimed to be compromised are Amazon Web Services, Duo, GSuite, OneLogin, Slack, VMware and Windows. Bleeping Computer additionally reported the attacker had accessed and taken data from Uber’s HackerOne bug bounty programme, which could be particularly dangerous for Uber if it contains undisclosed or unpatched vulnerabilities in its application."



vx-underground

[redacted]

Slack has been stolen, confidential data with Confluence, stash and 2 monorepos from phabricator have also been stolen, along with secrets from sneakers.

#uberunderpaisdrives

[redacted]

When the individual breached Uber, they sent a slack notification to everyone informing them the company had been breached.

Employees thought it was a joke.

Photo via ColtonSeal

Dúvidas?