ADDO

ALL DAY DEVOPS

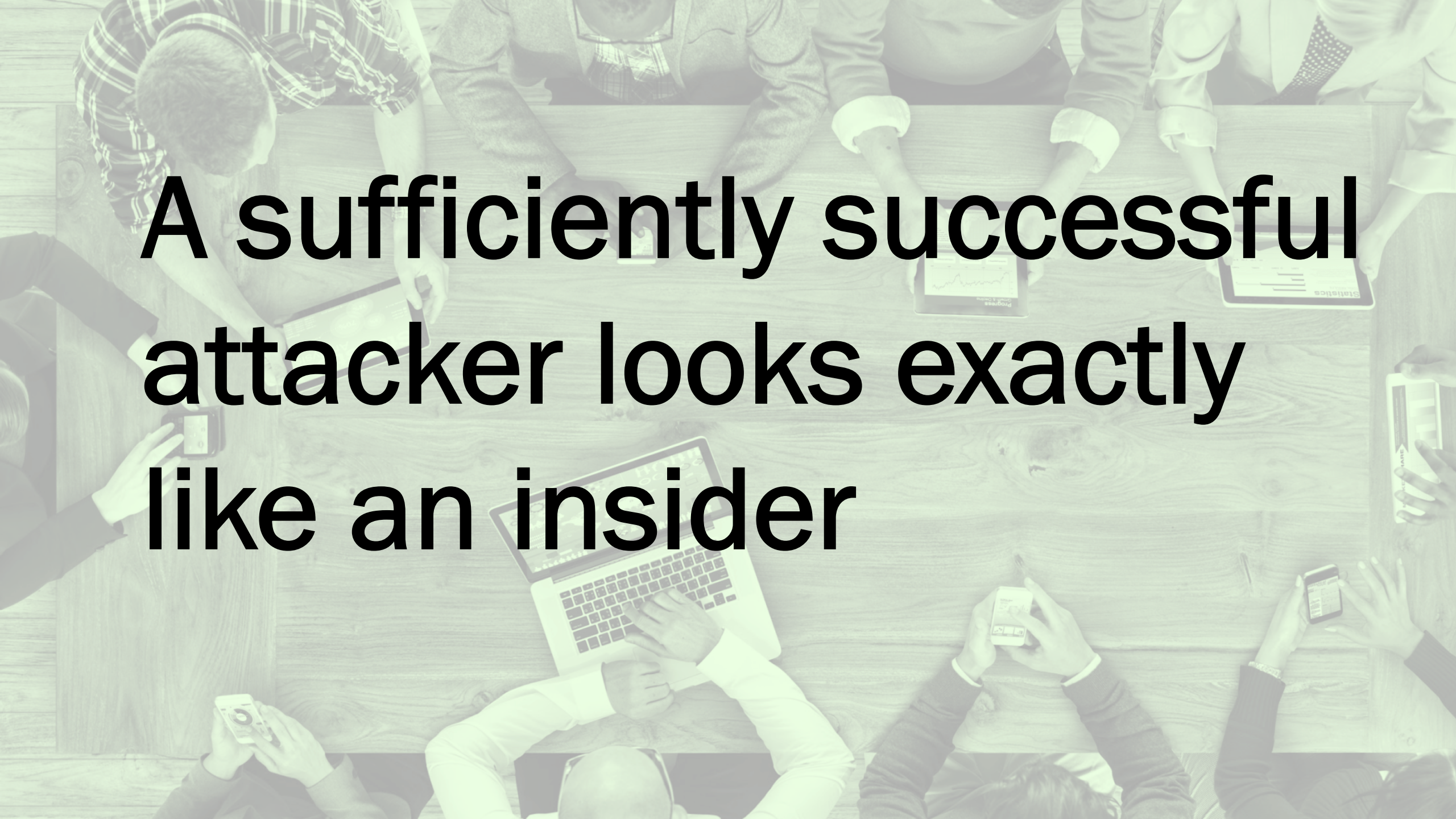
NOVEMBER 6, 2019

Wendy Nather

ZeroTrustOps: Securing at Scale

What does “zero trust” even mean?

What does “zero trust” even mean?



A sufficiently successful attacker looks exactly like an insider

Analogy:

Bouncers vs. Bartenders

How implicit trust is a problem

Colorado

COLORADO
Division of Homeland Security & Emergency Management
Department of Public Safety

Business Emergency Operations Center

Home | Donate Resources | Business Vendor | Business Damage Assessment | Recovery Resources | DHSEM

Activation Reports

After Action Report Released for CDOT Cyber Incident

Between February 21 -23, 2018, a threat actor executed a ransomware attack on that ultimately affected roughly half of the department's computers. Despite immediate action by the Colorado Department of Transportation (CDOT) and Governor's Office of Internet Technology (OIT), CDOT suffered a second attack on March 1, 2018. On March 3, CDOT, OIT, and the Colorado Division of Homeland Security and Emergency Management (DHSEM) formed a unified command group (UCG) to provide direction and control for incident responders. On March 8, the UCG completed phase one (Containment) objectives and shifted to phase two (Eradication) operations. On March 9, the UCG completed phase two (Eradication) objectives and shifted to phase these (Recovery) operations. Recovery operations continued for several weeks.

Read the full CDOT After Action Report for the 2018 Cyber Incident.

Trust assumptions

- “It’s only a temporary instance, so it doesn’t need the usual security configurations.”
- ”Nobody will notice this instance.”
- “We join everything to the internal domain, even if it’s not internal, because that makes everything operate smoothly.”
- “If you’re part of the internal domain, we don’t need to check you again.”

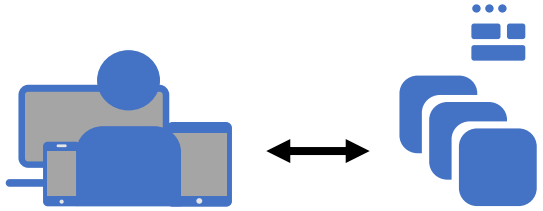
Wait, aren’t these just basic security principles?

Yes and no.

Different ways to apply zero trust

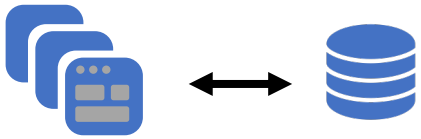
Think of the perimeter as being any place where you make access control decisions

Workforce, workload, workplace



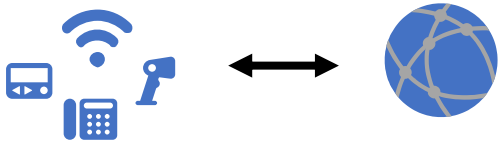
Workforce

+ Is the user who they say they are?
+ Do they have access to the right applications?
+ Is their device secure?
+ Is their device trusted?



Workload

+ What applications are used in the enterprise?
+ What is communicating with applications/data?
+ Is communication w/ the workload secure & trusted?



Workplace

+ Do users & devices authenticate for network access?
+ What access are they granted?
+ Are devices on the network secure?
+ Is their network segmentation based on trust?

	To Devices	To Apps	To Networks	To Data	To Users
From Devices	SSH certificates	Client-side TLS certificate Geofencing Fingerprinting	NAC	Encryption keys	
From Apps	Server-side TLS certificate	API key		Encryption keys	Enhanced TLS certificates
From Networks	802.1x certificate		Firewall rules		
From Data	Hashes/ checksums	Hashes/checksums			Hashes/ checksums
From Users	User credentials 2FA Biometrics	User credentials 2FA Biometrics	User credentials 2FA	User credentials 2FA	Photo ID Handshake

Source: Sounil Yu

	To Devices	To Apps	To Networks	To Data	To Users
From Devices	SSH certificates	Client-side TLS certificate Geofencing Fingerprinting	NAC	Encryption keys	
From Apps	Server-side TLS certificate	API key		Encryption keys	Enhanced TLS certificates
From Networks	802.1x certificate		Firewall rules		
From Data	Hashes/ checksums	Hashes/checksums			Hashes/ checksums
From Users	User credentials 2FA Biometrics	User credentials 2FA Biometrics	User credentials 2FA	User credentials 2FA	Photo ID Handshake

Reduce/eliminate these perimeters to make security more usable!

Source: Sounil Yu

ADDO
ALL DAY DEVOPS

What to pay attention to with DevOps

Impact and scale are different

- Users tend to be admins with elevated privileges
- Pay attention to inter-workload communications
- Automation can help and harm

Where will the attackers move next?

- If we prevent lateral movement within networks, they will probably switch to lateral movement between applications – so watch your APIs

Trust is neither binary nor permanent

- What do you trust them to do?
- What conditions need to be true?
- For how long?

ZeroTrustOps Guidelines

- Segment your stuff
  - Don’t let anything talk to anything else without a good reason
- Don’t assume someone else did the checking
  - Be your own bartender
  - Enforce your own policies at your layers
- Authenticate early and often
- Encrypt everywhere you can

Thanks, and good luck!