MK: Changes in the cybersecurity industry

Hi, I'm MK, Director in the Office of the CISO for Google Cloud.
The role of the Chief Information Security Officer is both to protect Google Cloud from a security standpoint.
But also to ensure that we're providing all of the tools and products necessary so that our customers can achieve their security outcomes as well.
So I spent a number of years in the US government, 32 years in fact, 22 of which were spent as a special agent in the Federal Bureau of Investigation.
About midway through the course of my career, I had the opportunity to shift into cybersecurity lanes, which initiated, or should I say, reinitiated my interest in all things computers and computer science.
One of the things that the industry lacks is a sense of agility, that the adversary has in spades.
When they identify something that works for them, they continue to pound on it until and unless there's an obstacle.
And then once that obstacle is put in their way, they have shown an ability to easily pivot their tactics and techniques so that they can bypass the obstacle in future attempts to gain access to environments.
And so none of us can predict the future.
We're not at any kind of final stage.
This is a continually evolving industry.
What you can ascertain is that we need to be prepared in a variety of ways to combat what will certainly be a persistent onslaught from the adversary.
What that requires is a certain sense of agility, you have to be comfortable in existing in the unknown.
But you also have to have the intellectual aptitude in order to be able to digest and formulate new solutions on the fly.
Zero Trust is a huge trend right now because it's both been a desire of the industry to move toward Zero Trust, but also a requirement in some areas around the world.
Zero Trust is a movement away from the historical way that we've done security in the past.
Layman's terms, so you're a business traveler, you travel with your business laptop and you check into your hotel halfway around the world, and you need to get prepared and ready for a business meeting that's about to occur.
Historically, you'd want to be able to attest to the fact that that is an intended or qualified user within the enterprise attempting to gain access to this information.
And yes, based upon the information that you have, the identity and coupling that with device information, that user and device should have access to this information and be able to make a determination about it.
I do believe that the more that we invest in the Zero Trust approach or architecture, it will get us to a good point from which to pivot off of.

But I think a lot of what's to come is unknown, and that means continual learning.
It means, continually exposing yourself to different parts of the industry so that we are prepared for what may happen in the future.

Revision #1
Created 2023-09-20 18:36:24 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai