How to practice cyber security and why it's different from IT security……

Cyber security isn't about one threat or one firewall issue on one computer. It's about zooming out and getting a bigger perspective on what's going on in an IT environment.

Keeping companies safe from attackers is no longer just a technical issue of having the right defensive technologies in place. To me, this is practicing IT security, which is still needed but doesn't address what happens after the attackers infiltrate your organization (and they will, despite your best efforts to keep them out).

I'm trying to draw attention to this topic to get security teams, businesses executives and corporate boards to realize that IT security will not help them once attackers infiltrate a target. Once this happens, cyber security is required.

In cyber security, the defenders acknowledge that highly motivated and creative adversaries are launching sophisticated attacks. There's also the realization that when software is used as a weapon, building a stronger or taller wall may not necessarily keep out the bad guys. To them, more defensive measures provide them with additional opportunities to find weak spots and gain access to a network.

This mentality goes against the fundamental principle in IT security of erecting multiple defensive layers around what you're trying to protect. By separating what you're trying to protect from the outside world, you're keeping it safe—at least in theory. While this works in physical security, where IT security has its roots, it doesn't really work when you're facing enemies who need to be successful just once to carry out their mission. Defenders, unfortunately, don't have this luxury. They need to catch every attack, every time. Don't take this statement as a knock against these antivirus software, firewalls and other defensive technologies; they're still needed in conjunction with cyber security.

Cyber security means looking for attacker footholds, not malware

IT security and cyber security also differ on what action to take after an attacker breaks through your defenses. In IT security, when a problem is detected on one computer, it's considered an isolated incident and the impact is limited to that machine.

Here's how that scenario typically plays out: Malware is discovered on the controller's computer, for example. An IT administrator or maybe a junior security analyst removes the machine from the network and perhaps re-images it. Maybe there's an investigation into how the computer was infected and a mis-configured firewall is identified as the culprit. So, the firewall configuration is changed, the threat is neutralized, the problem is solved, and a ticket is closed. In IT security, where the quick resolution of an incident is required, this equals success.

Now, here's how that same incident would be handled from a cyber security perspective. The team looking into the incident wouldn't assume the malware infection is limited to one computer. And they wouldn't be so quick to wipe the machine clean. They may let the malware run for a bit to see where it phones home and how it acts.

Most important, the incident wouldn't be seen as a random, one-off event. When you apply a cyber security lens to incidents, the belief is that every incident is part of a larger, complex attack that has a much more ambitious goal besides infecting machines with malware. If you close a ticket without asking how an incident or incidents are linked (remember, attacks have many components and adversaries commonly carry out lateral movement) or where else attackers could have gained a foothold, you're not doing your job.

To practice cyber security

Practicing cyber security begins with security teams changing their mindset around how they handle threats. To start, they need to be encouraged to not quickly close tickets and spend time looking for a full-blown attack in their environment. They also need to understand that cyber security isn't about one threat or one firewall issue on one computer. That view is much too myopic. Zoom out for a bigger view.

I admit this approach is a radical departure from how most organizations currently handle security. Further complicating this perspective is the fact that what I'm proposing can't be learned in classrooms or professional development courses. The notion of experience being the best teacher applies to figuring out cyber security. Step one is thinking like a detective and asking questions about the incident like why was this attack vector used, are there any strange activities (however minor) occurring elsewhere in my IT environment, and why would attackers target our organization.

It's this big picture thinking that separates cyber security from IT security. And it's big picture thinking that will help companies detect and stop adversaries after they make their way into an organization.

Dipl.Ing. Bernhard Bowitz

CISSP, BSI 100, 27001