Digital Distancing

A Spotlight Interview with Tom Kellermann

"While a VPN is not a silver bullet, it should be used when accessing trusted assets over untrusted networks."

TOM KELLERMANN
HEAD OF CYBERSECURITY STRATEGY
VMWARE

Meet Tom Kellermann

Tom Kellermann is the Head of Cybersecurity Strategy for VMware. Tom serves as the Wilson Center's Global Fellow for Cybersecurity Policy and sits on the Technology Executive Council for CNBC. In 2008, Tom was appointed a commissioner on the Commission on Cyber Security for the 44th President of the United States.

Q: You've recommended 'digital distancing' as a way to mitigate the threat of island hopping and proximity-based attacks (e.g. jumping from smart home devices to corporate-owned ones).

What recommendations do you have for employees who may live in shared housing spaces (e.g. group homes) with limited privacy or control?

A: Even if you are sharing a house, or don't have root access to your home router, you can still take precautions to protect yourself. So, the first thing is to make each of your devices less of an easy target. Imagine you had to walk through a sketchy neighborhood. You wouldn't take all your important keys with you. For example, the key to your house, your office, your safety deposit box, your car, your storage unit, all along with each address written on each key. This is sort of like the equivalent of setting up at least two profiles on the device—so that when remote workers are accessing untrusted networks they use the profile that has the least amount of privilege. In general, it's a good idea to turn off administrative privileges on the device.

Make sure they're updating all of their applications and OSes, and in particular that they've installed EDR and NGAV and keep it updated as well. While a VPN is not a silver bullet, it also should be used when accessing trusted assets over untrusted networks. Another recommendation is to use Firefox as their default browser, since it's more secure than most mainstream browsers.

Q: How can IT security teams best maintain close coordination in thwarting attacks while they're sheltering in place at home, away from the SOC and each other?

A: Number one is they should have regular conversations over an outside mechanism like Slack. Conduct a daily briefing regarding active cyber threats that are facing the organization or threats that are impacting other entities within their industry. Run weekly tabletop exercises for these threats and discuss how to deal with these phenomena. Use these to inform a proactive threat-hunting program to find attackers operating under the radar, combined with good cyber hygiene to continually reduce your overall risk surface area. All of these are the tactical steps needed for IT security teams.

Dwell time = the amount of time an attacker operates on your infrastructure without your knowledge.

But the real game changer is in integrating the control points across your enterprise so that you can defend in a holistic way—that is intrinsic security in a nutshell. Coordination of every control point results in a self-defending enterprise security strategy, one that can scale to meet each and every innovation coming from the attacker side.

One more point about SOC teams. Mental health has never been a strong suit for cybersecurity warriors. Between long-term burnout, and the collective feeling that we're losing a war and facing an insurgency, we must be more mindful. Organizations should allow for more flexible schedules and provide support in new creative ways. IT security pros have needed to serve during some tough times, these are some seriously tough times.

LEARN MORE

THE FUTURE OF REMOTE WORK: SECURING A DISTRIBUTED WORKFORCE EBOOK

Check out our one-stop-shop eBook for everything you need to know about workforce security, so your users (and you) stay safe while working remotely. After all, the easier you make it for employees to do the right thing, the better the outcome. *carbonblack.com/resources/the-future-of-remote-work-securing-a-distributed-workforce*

Q: Attackers use many methods to maintain a persistent presence on a network, including adding C2 channels, and patching any vulnerabilities they used to gain initial access. If we can no longer measure the effectiveness of our security program by how well we keep the bad guys out, what should be our new measuring stick?

A: Attack prevention is not the measuring stick anymore and that's due to a number of things like fileless malware, living off the land attacks, combined with the wide distribution of the best cyber weapons produced by the U.S. government after the Shadow Broker breach. The reality is that the attackers are already there on your trusted infrastructure attacking you from the inside out. In fact, more than one-third of data breaches involve island hopping.

Dwell time is the new metric. How fast did you contain the last breach and divert that adversary without them knowing? Remember: decreasing dwell time in a clandestine fashion is the goal. By the way, if you're wondering why you wouldn't want to simply kick the bad guys out of your network right away, there's a very important reason.

More and more adversaries are leveraging wiper malware or ransomware 'NotPetya style' without ever asking for ransom. Inside your infrastructure, they can do significant damage, wielding this threat and power as a form of counter incident response. That's why decreasing dwell time in a clandestine fashion is the name of the game. And the only way to do that is via intrinsic security—when you can coordinate defenses across all of your control points, neutralize the threat quickly and thoroughly before an attacker is ever tipped off or kicked off.

Q: We've talked about 'digital distancing' as being a good analogy for social distancing. Is there a cybersecurity equivalent for hand washing? If so, what would it be - for both remote workers and the enterprise?

A: For enterprises, good cyber hygiene includes the capacity to audit the current system state, as well as immediate visibility into behavioral anomalies which is what EDR offers. For remote workers, it's about patching your apps, your OS, ensuring that NGAV is running and is up to date especially when you're accessing sensitive information, whether that's personal finances, personal communications with loved ones, or doing a telehealth session with your doctor. Before you do any of those things, make sure you don't have a lot of browsers (and tabs) open, and only use the one application that is required for that purpose. People often forget that there's a bidirectional flow occurring across all of those channels that can bypass encrypted tunnel security.

Remember, at the end of the day, the game has changed. The worst-case scenario is a much bigger nightmare than we've ever faced before—both from an enterprise perspective as well as an individual one. We need to revisit our assumptions, and design risk management strategies that reflect this new reality.