ALLIANCE Media Group

Alliances

Digital Alliances

continue collaboration

CISO Alliances – UK&I
23rd September 2021

In Partnership with :

cisco SECURE

Alliance - ‘A union formed for mutual benefit’

DigitalAlliances

continue collaboration

ALLIANCE Media Group

Food For Thought/Topics Discussed

Session Leader:
Xavi Garcia Faura, Cloud Security Leader – Cisco
Martin Lee, Manager, Talos Outreach EMEA & Asia – Cisco
Session Title:
Adopting the Attacker's Mindset to Protect the Hybrid Workforce
Session Synopsis:
The hybrid way of working is an established reality and one which has opened up a host of opportunities for criminals. Attackers no longer need to execute direct attacks, using attack vectors targeted straight at systems or at individuals. They can now take advantage of the supply chain in order to spread out the attacks elsewhere. In this new reality, you have to think like the attacker to avoid being the next victim.
What new tactics are criminals employing and how are they distributing attacks to take advantage of the hybrid model? What is being overlooked in our current defences? How are the attackers succeeding despite our defences?
Register for this executive roundtable for new insights and discussion about:
Defence strategies to protect the hybrid workforce
Recommendations to achieve greater threat coverage and visibility of attacks
Trends to watch in 2022
Adopting the attacker's mindset

DigitalAlliances
continue collaboration

Food For Thought/Topics Discussed

cisco SECURE

Community Questions/Comments

- Fundamentally there's two ways that we can hunt for threats. You can either look for anomalies within the data. So we spend a lot of time looking at telemetry, slicing and dicing the data in various different ways to identify what's wrong. The other way is to spend a lot of time thinking about, if I was an attacker, what would I be doing? And to start thinking, if I was going to attack a system using this particular technique, what would the traces be?
- With more people working from home or even hybrid working (office & home) working, there is a high possibility that you or family members are using the same laptops/computers that are used for work are being used for homework, searching the internet, playing games.
- With this information we can start to think as the attacker and how they would use this information to attack.
- What have you seen, and what experiences have you had in working remotely and working with a remote workforce and, what attacks have you seen that otherwise you think that you might not have?
- When the pandemic hit us, we took a decision very, very early on that we did not want to address the risks of homeworking. We didn't want data going home. We didn't want data to be printed out anywhere. We didn't want any issues with people not having laptops necessarily. So they couldn't take them home and then taking desktop.
- The threats that we saw, we didn't really care about them because we knew that if everything is going over web browser, multifactor authentication for login, there is no way anyone can do anything with that.
- You massively reduced the attack footprint, like having a BVI infrastructure. And that is now enabling people to work from anywhere on anything at any time






Food For Thought/Topics Discussed

cisco SECURE

Community Questions/Comments

- We had some very unique challenges. And actually one of the biggest challenges we had was, was a physical challenge in the fact that the majority of our employees globally are geophysicists and geoscientists, because they're manipulating a very large, very high resolution images. So we actually had to send their desktops out to them at home.
- We did a study looking at who was, or which job role was most likely to be sent, targeted attacks over email. And interestingly it ended up being senior engineers, geophysicist in the oil and gas industry was a job role that was very, very high risk of getting a targeted attack.
- Talking to a pharmaceutical company, um, a few years ago and, they adapted very much to the philosophy that everything that we do really should be source, our scientists are publishing in the journals. We want, actively want our scientists to publish in the journals because this is promoting our medications. And they're all protected by Paton anyway. So if you stole our raw data, actually this wouldn't help anyone. And for them the risk was more ransomware of no longer having access to the raw data, but actually having that data in many places. And even if it, if it leaked, that wasn't so much a concern of theirs, which I thought was quite interesting.
- That's absolutely compatible though, with a good information security posture, right? You protect the high value assets, you protect things which are the biggest list of the company.
- One of the things that struck me about the conversation so far is all of the conversation has been quite mature in terms of it's risk-based approach, it's something that you don't see often. I have talked to a lot of customers over the last 10 years or so. And the ability to sit and in quite cold terms, analyse the risk posed by these different ways of connecting these different scenarios, isn't something that I think has been massively prevalent across the customer base that, that I've dealt with.

Food For Thought/Topics Discussed

cisco SECURE

Community Questions/Comments

- The mature risk based approach is one of the things that the pandemic probably has shifted because it wasn't something that people could choose to do, it was was driven that they have to do, and therefore they have to take those steps very quickly. The pandemic has driven quite a lot of changes in approach very quickly, that otherwise the industry probably would have got to but at different paces.
- The whole hybrid working from home has demonstrated that if you do the security right, then you'd be an enabler to the business and it, and it has helped organizations take that step and make that shift.
- One of the big problems is retrieval, people leave organization and how do you get assets back? Because people are not motivated to give you the asset back. That in itself is a very different kind of security challenge.
- I firmly believe that if you do identity well, which is one of the hardest things to do, then you can mitigate a lot of these other risks.
- This has been happening for a while, but fundamentally we've got down to the point where all your organizations actually are interested in or need to be focused on is giving the right people access to the right data at the right time.
- Fundamentally if you can connect the right people to the right assets at the right time, in the right way for the right reasons, then we're getting towards the sort of tools understanding that. You start getting back to understanding how to see how your business works. And if you do that, a really good understanding of fundamentally how your business works and what they need to do, but that's a really good starting point.

Food For Thought/Topics Discussed

cisco SECURE

Community Questions/Comments

- Customs is another issue when it comes to retrieving hardware from employees, whether that be laptops being sent back from employees working in different countries or when deliveries get stuck.
- Sending laptops out to new starters has been incredibly, incredibly challenging.
- Thoughts on password less?
- It's the direction that technology is moving in, ever since apple started, the whole drive of technologies to make it more easier, more seamless, the biggest challenge is going to be cultural with this.
- It's a cultural problem. Take it slow and it will come and just have the solutions ready for when it's ready for, for mass market.
- We are already playing with it to see how we can break it. We're already using 3d home printer to print fingerprint molds.
- Certainly a sophisticated attacker would be able to replicate your fingerprint and we are also looking at the 3d face scans, and thinking how can we fool those? Can we print a 3d image, a mini head, that you can put up by a camera to fool it.
- If your password is compromised, you change it. If your face ID is stolen, what do you do then?
- There is also the issue of if you have an accident where you may not have finger tips or face altered then if we are just purely password less, what happens then?
- We will always have to have that secondary source to combat these unusual issues.

Feedback

- Great session, thank you.
- Very insightful conversation today, thank you.
- Thank you Martin, cracking conversation and points. A lot to think about and digest.
- Great discussion points, nice to have a discussion without PowerPoints.