Beyond
Zero Trust

Hello everyone,

So, moving away from my more philosophical posts, let's talk about what I am really good at... being technical.

And before you think "Snore" and start scrolling - I'll be keeping the technical details to a minimum and you can do your own research or speak to us after you've read what I have to say

The absolute basics of good security posture

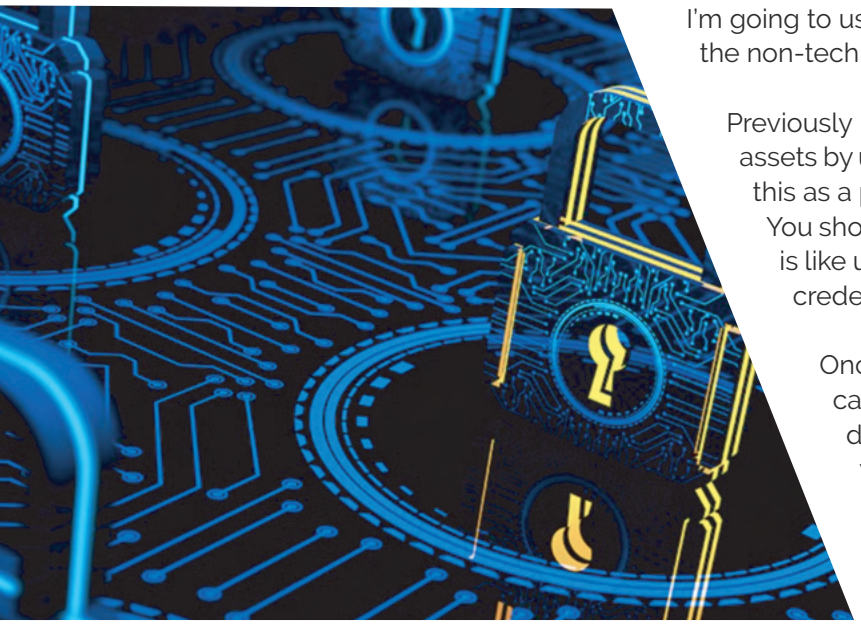
We all know cyber security is a massive deal, without it your organisation will not survive day-one on the internet. You know that you must keep your passwords safe and to keep changing your password often. That doesn't mean on a sticky note attached to your monitor - you know who you are!

You know sometimes you must enter a code that gets sent to your mobile, which is annoying, but the kid from IT said you had to.

You also know that you should be cautious of fake emails from the CEO asking you to go and buy 10 amazon gift cards on the company credit card and send him the codes (Yes this has nearly actually happened, but thankfully the codes were never sent).

But I bet you didn't know that what you might have considered 'great cyber security' 5 years ago, could now be a huge risk.

The Security Perimeter



I'm going to use a metaphor to interpret the technical concepts, so the non-technical folk can understand also.

Previously organisations ensured the security of their data and assets by using the 'security perimeter' model. You can imagine this as a private event with tight security around the building. You show your invitation and the security team let you in (this is like using your key card to enter the building or using your credentials to VPN into the office network).

Once you are past security you considered 'trusted', you can go and talk to whoever you want, grab yourself a drink and people are happy should be there because you managed to get in.

Of course, this 'Security Perimeter' model worked very well, your key card or credentials were enough proof of who you are.

The flaws in the model

But nowadays, most people aren't in the office; some people don't even use a computer a lot of the time.

Your work can be done remotely through your phone on the other side of the world while sipping a mojito. On top of that you might not have even connected to the office, as the data is now in the cloud, and you can work from your browser.

These newer modern methods are brilliant for productivity and now considered a 'must-have' for almost all organisations. However, they also present an additional problem to security by opening your company to many more attack vectors.

Going back to the metaphor, you can consider this modern way of doing things is like an open (outdoor) event.

Anyone could walk in from the street and pretend to be part of the staff, go a grab a drink without paying, collect information not meant for them or steal some chairs for their own event.
Sure, you still have a perimeter but there a too many routes into the event, and the 'security perimeter' is now not sufficient for the event.

Zero Trust

Introducing the ZERO TRUST model, where no one is trusted by default and MUST verify who they are, every time.
So now, everyone who was invited to your open event is given a lanyard with their event pass.

If they try to grab a drink, they must show their pass, and the bar tender can keep track of who got a drink.
If they start talking to someone, they must show their pass, by default no one will talk to someone without a pass.
If they try and walk off with some chairs, unless they have the right 'permissions' on their pass, then someone is going to stop them.

The Zero trust model follows 4 main concepts that you should always keep in mind.

- **Never Trust, Always Verify**
- **Least Privilege and Default Deny**
- **Full Visibility and Inspection**
- **Centralise Management**

As an added bit of knowledge to link in with the 'event' metaphor, if you have ever heard of SSO or 'Single Sign-on' this is akin to having the event pass stuck on your forehead the entire time.
No need to have it checked every time you get a drink, the bartender knows you are part of the event, speeding up the whole process.

I hope you enjoyed the metaphor and it helped explain the concept.

If you need any help with your security assessments or ensuring your acquisition integration proceeds without introducing risk - we are here to help!

Visit us at https://www.beyondmigration.com/services

Author
Lewis Evelyn
Technical Delivery Engineer