Digital Defence: Investing in IT infrastructure to defend London's public transport infrastructure.

Paul Graziano is the 'Cyber Security Investigations & Threat Intelligence Manager' at Transport for London. In this interview, Rory Hanna from our Marketing Team at Logicalis talks to Paul about the role cyber-security and compliance has to play in protecting and defending critical public infrastructure.

TRANSPORT FOR LONDON

Paul Graziano - Cyber Security Investigations & Threat Intelligence Manager at TFLL

Paul is part of the Security Operations team and looks at maintaining and improving the security and visibility of this critical national infrastructure and its industrial control systems.

Defending the UKs largest public transport network through innovative approaches.

Rory: Hi Paul, lovely to meet you, why don't you give us an Introduction?

Paul: My name is Paul Graziano, I've been working at TFL (Transport for London, a not for profit organisation) for about 18 months so far, and I'm involved in deploying the Security Operations centre. That was my main role within the first ten months, where I was solely involved in the information technology side. I think within the past 8 months the operational technology information side has become the most interesting aspect of my job so far. This includes the whole crucial, critical national infrastructure and industrial control systems. The last 8 months has been about increasing visibility on these parts of the system so we can monitor them and alert ourselves to anomalies appearing in these systems therefore detecting suspicious activity, I'll touch on this further later.

"The age old issue with security is that the devices we rely on, were built in a time when security wasn't really an issue".

Rory: The transport system is part of our critical national infrastructure - how do you see the cyber threat against our critical infrastructure evolving?

Paul: Good question, so I think cyber security within critical national infrastructure is becoming an increasingly complex task, this is for a number of reasons; firstly, like the age old issue with security is that the devices we rely on, were built in a time when security wasn't really an issue. So they were

designed to be in an air gap system, an off the grid network where only a few number of people would have access to them but now more and more modern industrial control systems are being connected better by IT Infrastructure. So that's central management, improving efficiency, these are all obviously better positive things but it means we don't design ourselves in a position where we have to break in security to protect residency devices, which is what we're currently working on. In most cases the Let-you-see systems don't have the security capabilities, so we need to deploy upstream security capabilities. Instead of having security by design, we need to put the monitoring around these systems, so we know what users are accessing, know what they're doing as well as the network monitoring around these devices too.

Rory: What can we do to protect our critical infrastructure against attack?

Paul: I guess there's no simple answer to this, I think in some ways what we're trying to do now is use a framework we've adopted in Information Technology (IT) to protect Operational Technologies (OT) which involves a security strategy, this is a cradle to grave strategy. Security needs to start right from the beginning of the procurement of these new systems and they need to make sure any new systems meet our security requirements, essentially auditing and monitoring. Most importantly, this ability needs to be fed back into our Security Operations team, so I think we just need to assume that we will be compromised. As long as the Security Operations team have that visibility we will be able to respond to any incidents if need be and they'll also need to be able to pull the plug in worse case scenarios. We have tried to create a parallel to what we've done to protect our IT Infrastructure. In terms of specific advice for crucial, critical, national infrastructure, there's the CPNI, a UK government body, (aka 'Centre for protection of National Infrastructure') and they release a number of frameworks for industrial control systems. It is referred to as 'CPNI sics' (the 'sics' stands for 'security and industry control systems') and they set up 10 principles. They believe we should structure our industrial control systems to make them secure and deploy frameworks around them to achieve that. A lot of work has been within the government to help us out. So we've got that side of it as well.

"Security threat intelligence in particular has become more and more important"

Rory: What are your thoughts on the value of threat intelligence and security analytics in the fight against cybercrime?

Paul: Both are an extremely, extremely important part of Security Operations, they are key vital parts to it. Security threat intelligence in particular has become more and more important, we're always going to be playing catch up and so we need to have a foot in the wider world. We need to understand what's happening, what the new threats are, we need to not just look at our key assets, obviously that's very important to do so, but also understand what the wider threat to the rest of the world is and how that could morph into attacking TFL or any particular company. Security analytics is incredibly important, that's what I've been working with the SOC team to get that capability, so it's the most important part for any cyber security team, to protect your network you need to have good visibility over it. You need to know what's going on and you can only really achieve that through security log analytics and you need to have the capability to sort logs from all these number of sources and correlate it for suspicious activity, so you benchmark it to understand what normal looks like and then you look out for anomalies. I think just due to the volume and the speed in which they're coming in, all of this needs to be automated. The security team also needs an analytics solution to be able to do a lot of that work for them and just present them with the alerts for suspicious activity, I think that's when they come in and triage the alerts to confirm whether it's malicious.

"With every device that is IOT they're being targeted for BOTNET activities"

Rory: Will the Internet of Things significantly change the way you address cybercrime?

Paul: Yes, absolutely. Obviously with more and more devices being connected to the internet. At the moment it's just from the commercial side, like driverless cars, and more and more mobile phones but that was always going to find its way into the business side of things. It already is with IP-CCTV that you have components that are a key and critical part of the business being connected to the internet and we need to ensure they're secure and that they have the appropriate security requirements around them. With every device that is IOT they're being targeted for botnet activities, again they are not inherently secure so they're easily targeted to be able to take over those devices and then just help them be part of a larger attack, so yeah it is a very difficult problem to solve and we can't be isolated as a business in dealing with it, there needs to be a consolidated effort.

Rory: How are you using virtualisation to transform your business?

Paul: The TFL are hugely into virtualisation so I think a really good example of this would be TFL.gov.uk, our public facing API, that's used for TFL's journey planner and it powers applications like Citymapper too. We use AWS for these cloud technologies which is essentially the same thing as virtualisation, we just don't host the virtualisation servers ourselves. In terms of how it's changed our business, its changed the way in which we think about new projects and new applications because we can easily build rapid prototypes for new applications and we can test whether they work or not relatively quickly with very little cost where we

haven't been in a position to do that previously. Now we don't really rely on purchasing and racking up a new server every time we start a new project which is a very good thing. I think it also gives us a lot of flexibility too, we scale up pretty much automatically when we need to, and it's not something we really don't need to think about anymore with virtualisation, it just happens. You need to configure it yourself but once you have configured it then it looks after itself. Again, we would never have been in a position to do that before virtualisation. There is a renewal aspect to it too, that if configured correctly, it's relatively simple to spin up a new server if your prime one goes down. So there are many great benefits to virtualisation.

"Virtualisation means it's relatively simple to spin up a new server if your prime one goes down"

Rory: How are you providing security and visibility into this environment? Are you using technologies such as micro-segmentation (e.g. VMware NSX)?

Paul: Yes, good question. I think we have a security based designs approach, so fortunately we like cloud based technologies because they're like new services which we've been enrolled in right from the beginning. The threats which cloud and virtualisation pose to traditional infrastructure, they're relatively the same but its amplified by how quickly you can set up new servers, how easy it is for you to change firewall and open up to the network, so these risks have always existed but we just need to be able to catch them quicker because they're happening quicker and the only way you can do that is security by design, so again security log analytics, we need to ensure we have visibility over our virtualised environment, so you can understand who has access to them, who can set up servers, when if servers have been set up we need to know straightaway and again the security routes as well. Micro segmentation security groups pretty much cover that. So we need to make sure only servers which need to communicate with the appropriate servers can do so and so we need a policy in place as to what can happen and if anything defers from that policy then we know about it and can chase it up.

Rory: What other technologies would you suggest adopting in the fight against cyber-crime?

Paul: So maybe first thing, not so much a technology but more like an awareness strategy would be useful, if you look at the number of the high profile attacks over the last year, a lot of them started with simple phishing attacks, so again, as with everything else we're always going to be playing catch up with phishing. Our spam filters will never be able to spot the first email (from a spammer) from a newly setup phishing campaign and they're purposefully designed to do that. One of the only ways to protect against that is to ensure our users are sufficiently trained to detect suspicious emails, not just to detect suspicious emails but how to respond to emails in general so we have a disclosed combination of information, opening attachments or running executables. I mean these are very, very simple things but they always seem to be the first level of attack for some reason. I think the only way you can solve that is awareness, making your employees aware of the impact it could potentially have if they do this wrong. In terms of an actual technology, I think privileged identity access management is also key to a security team, so you need to understand who has access to the most critical parts of your business, which users have that privileged access and during a compromised attack, hackers will look for the businesses crown jewels so to speak, and who exactly has access to them.

"The only way you can solve that is through awareness, by making your employees aware of the impact it could potentially have if they do this wrong."

Rory: So you mentioned a change in practice and policy that a company needs to instigate because unfortunately a lot of these first wave attacks happen due to poor user practices. You did mention one piece of technology there wherein certain individuals have clearance so as to minimise risk of attacks on the business by reducing accessibility. What other technologies would help in this fight?

Paul: So I think that one of the technologies that the industry is looking at more widely is called 'deceptive security technology', that is essentially a very old security component called a 'honeypot' where you commercialise a 'honeypot'. These are systems that are built to be insecure and placed in a public part of your network. By doing so, you can see who finds it and what they do to it, to understand what threats are being taken out on it and then you will get a wider picture. It is essentially threat intelligence to be honest. Proactive threat intelligence to find out if people are attacking parts of your network.

Rory: Thank you very much for answering all our questions Paul and we wish you a fruitful career at TFL.

Thanks to Transport For London & Paul Graziano - Cyber Security Investigations & Threat Intelligence Manager at TFL.

© Logicalis 2017. All trademarks are acknowledged.