Keeping PACE with the changing threat

A point of view

Security is changing because the threat is changing. You need to keep rethinking the risk. You need a security approach that keeps PACE: one that's Proactive, Adaptive, Collaborative and Experienced.

Stop reacting and start anticipating

It's no longer enough to follow cyber crime trends and react to them. You need to be constantly monitoring and anticipating threats, because these days the stakes are simply too high not to.

Security is a massive problem – and we only see the tip of it in the public domain. Around 600,000 Facebook accounts are hacked every day, and in 2014 identity theft happened every two seconds in the US[1]. Meanwhile, 93 per cent of large organisations have experienced at least one breach in the past year[2].

It's also a very expensive problem. The World Economic Forum says "Data is the new oil" because it's so valuable. The Cabinet Office has estimated that cyber crime costs the British economy £27 billion a year[3]. The Distributed Denial of Service (DDoS) attacks on Yahoo and others, in 2000 were estimated to have a cost over $1.2 billion in damages. Sony spent more than $170 million cleaning up after their DDoS attack in 2014[4].

And it's going mobile. For 74 per cent of IT directors, security of mobile devices is the single biggest concern. Yet despite the rise of Bring Your Own Device (BYOD) only 36 per cent of organisations have a mobile security policy they enforce, leaving IT directors struggling to keep control[5]. And while the cloud opens up increasing opportunities, it also opens up bigger security risks, with around a quarter of security breaches happening in the cloud[6]. And older, non-cloud systems aren't much less vulnerable, either.

Security is also growing exponentially with the Internet of Things. Marc Goodman, Interpol's senior advisor on cyber security, estimates that another 200 billion devices will be hooked up to the Internet by 2020. "Computers are all around us" he says, "the electricity grid, the tube, the transport network, the car you drive – and like all computers, they can be hacked." And as if all this weren't enough, the risk is in your people too. You can have the best technology in the world, but if your people don't have a security culture, policy and training, breaches will still happen.

So you need an approach that keeps PACE

PROACTIVE

It's never enough to react to an intrusion. It's not even enough to detect it. You have to defend against it to stop it happening at all. To do that you need to know two things: where your vulnerabilities are, and what techniques hackers are using to exploit them. You need to continuously assess your vulnerabilities and monitor the evolving threat landscape. We've developed an ethical hacking centre of excellence and a threat intelligence service to do this.

But because security is about people too, you also need policies, training and internal communications, especially around mobile and BYOD.

ADAPTIVE

You need security capabilities that evolve and adapt, just like the threats they protect you from. You need to be able to capture, analyse and visualise big sets of security data in real time, especially when you find yourself attacked on multiple fronts at once.

To meet cloud-based threats you need cloud-based security. That's not just security for your cloud service, but security which is itself a cloud service. As with any cloud service, you can flex cloud-based security up or down easily. Also, you only pay for what you use instead of tying up capital, and you can tap into a wide array of skills to keep you completely up to date.

COLLABORATIVE

We all like to think we learn from our mistakes. But wouldn't it be better if we could avoid making them at all by learning pre-emptively from others? Cyber intelligence is increasingly collaborative. Organisations in both public and private sectors are coming together to pool intelligence and share best practice. The Government-led initiative CERT UK is one example of this in action. We provide threat intelligence services, and have done so for a very long time. It's this type of collaborative approach that will help to create a more complete picture of security threats and how they're changing.

EXPERIENCED

You can get access to scarce skills and deep experience by partnering with specialist outside providers. They offer scale and flexibility as well as knowledge of how threats are evolving as a whole. Comprehensive monitoring isn't something any organisation can really do in isolation. Outside security specialists build up experience of a wider variety of attacks than any single organisation sees, so they become more expert in countering them. They also employ very highly skilled specialists, which most organisations couldn't justify.

Embedding security at the heart of your organisation

We embed security into the heart of both our services and our customers' organisations. Every organisation needs a security partner who can help them to keep rethinking the risk.

To protect our own network and some of our most demanding security customers, like the UK Ministry of Defence, we've developed one of the best security practices in the world. We've turned our expertise into award-winning commercial services that other organisations can benefit from.

You can take advantage of our investment in technology, partnerships, skills and expertise. We share security information and threat intelligence with our partners so we can all identify and keep pace with emerging threats.

That's why we've developed services that have the right characteristics to address the problem as we see it:

ASSURE CYBER

A new all-in-one security platform that offers organisations comprehensive monitoring, detection and protection against cyber threats. It puts threats into context and prioritises them. It analyses the norm, so you can spot anomalies quicker.

ASSURE THREAT INTELLIGENCE

A service which gives our customers intelligence drawn from multiple sources on potential threats that may affect their organisation.

ASSURE ANALYTICS

A real-time big data analytics and threat visualisation.

ETHICAL HACKING

Teams who try to breach your defences before the real hackers do, and recommend what you need to put in place to protect what matters most.

Every month we block two million viruses and prevent five million suspicious (and 250,000 definite) attacks on our infrastructure. Our security for the London 2012 Olympic and Paralympic Games communications network stood firm despite as many as nine million attacks a day.

A strategic security partner

You need to join forces with a strategic security partner who can:

1. Make you part of a security community that gives you shared intelligence
2. Monitor and prioritise threats in real time
3. Equip you to defend against multiple attacks at once
4. Counter cloud risk with cloud-based security
5. Embrace the human factor - security is about culture not just technology
6. Give you outside specialists with wider experience and heightened skills

If you need help in rethinking your risk, or you want to discuss any of the issues we've raised, get in touch with your BT account manager.

> "The traditional security perimeter has dissolved. Cloud computing and mobile devices have the potential to make organisations more efficient, but they also introduce new risks. We help organisations master the changing cyber threat landscape - protecting data and applications in this new perimeter-less world."
>
> **Mark Hughes, president of BT Security**

[1]Bloomberg Business: Everyone wants a piece of your data

[2]BT Mastering the Threat Landscape

[3]The Cost of Cyber Crime, Detica Ltd and The Cabinet Office, 2011

[4]Ronen Kenig, Radware.com

[5]Both statistics, BT Mastering the Threat Landscape

[6]BT Cloud Research Findings pdf

Offices worldwide

PHME 74760