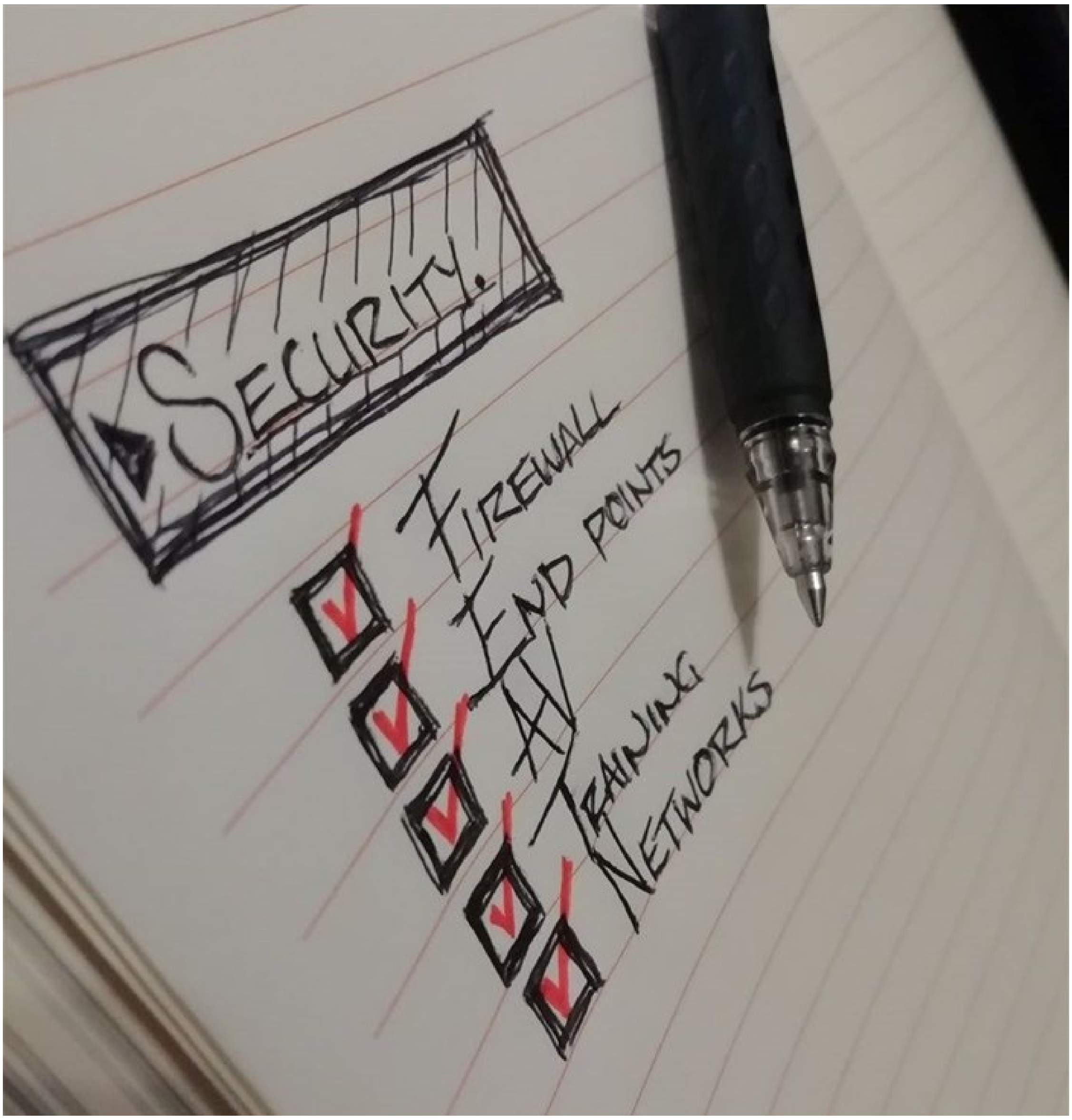
Avoid following a tick-box approach in your DDoS defences

Following a tick-box approach in business is not always a good thing.



While we can see the value in marking off checklists with regards to workplace safety procedures, as one example, the corporate equivalent of crossing off a to-do list doesn't always drive the business in the direction it needs to go.

And from an IT perspective, following a tick-box approach definitely has its drawbacks when it comes to mitigating distributed denial of service (DDoS) attacks.

This is according to Bryan Hamman, territory manager for sub-Saharan Africa at Netscout Arbor, which specialises in advanced DDoS protection solutions.

Hamman says, “Project management consultants maintain that ticking off checklists are not necessarily affecting the business in a positive way, but can instead serve simply to facilitate the apparent accomplishment of a number of deliverables that look good on paper. To avoid implementing a tick-box approach, it is key to ask: ‘Does this help the business?’

Certainly, the same question can be applied to important IT issues, such as ensuring that your business doesn’t get taken offline by a malicious DDoS attack that floods your system and causes it to slow down or crash.”

Assess where you stand

A recent Netscout Arbor blog entitled “Are you prepared for DDoS? (Not a checklist)” advises, “Instead of checking off a list of solutions, enterprises need to assess where they stand on a continuum of risk posed by DDoS threats.”

The blog notes that data from the Netscout Arbor Worldwide Infrastructure Security Report (WISR) for 2018, its 13th annual report, presented the following facts from the respondents who took part:

- 82% of the participants identified firewalls as a security measure that they had in place.

- 57% had intrusion detection/prevention systems (IDS/IPS).

- Only 28% had intelligent DDoS mitigation systems.

“As the blog points out,” says Hamman, “firewalls and IDS/IPS do have their place in the security arsenal, but they are inadequate against attacks intended to deny service. When security decisions reflect a tick-box approach, we find questions being asked like ‘What tools do we need to have?’ and ‘What do the regulators say we must have?’ But ticking all the boxes in order to be compliant can unwittingly leave an organisation vulnerable. Compliance does not necessarily equate with security. This is why the real questions that need to be asked are around identifying the DDoS risks that are being faced, and the preparations that need to be put in place against them.”

Protect against all threats

Hamman advises that a business needs to protect against all types of potential DDoS threats, namely: volumetric DDoS attacks; TCP state exhaustion attacks; application layer attacks; multi-layer, multi-vector attacks; outbound attacks from within, and emerging threats, which require a global threat intelligence capability.

“It simply isn’t plausible to try to cherry-pick which type of DDoS attack you choose to protect yourself against. Ignoring any of them will mean that at some point, your organisation is exposed to a threat. This is why Netscout Arbor advises the implementation of a hybrid or layered defence, combining cloud-based and on-premise detection and mitigation, which is powered by automation and informed by global threat intelligence alerts.

“If your IT professional feels that the organisation has bandwidth and/or budgetary constraints in terms of comprehensive DDoS protection, then exploring a managed DDoS service option will give you access to specialised DDoS protection and allow you to let the experts decide what is best for your business. It reduces your risk burden for the maximum budgetary effectiveness, and is driven by security experts who know which are the correct questions to keep DDoS threats at bay,” concludes Hamman.