datacentrix

How to mitigate (and recover from) rising African cyber incidents

By Brian Smith, Business Unit Manager, Datacentrix

There's no question that African businesses are being increasingly targeted by cyberattacks, with ransomware, spyware and backdoor incidents, as well as data leaks, becoming ever more prevalent.

One such recent example is the Distributed Denial of Service (DDoS) attacks on Kenyan and Nigerian organisations by 'hacktivist' Anonymous Sudan during July and August this year.

According to a report by cybersecurity company Cloudflare, the original group emerged in Sudan, “in response to the country's ongoing political and economic challenges. They were also known for using digital activism, which includes hacking and DDoS attacks on governments and other high-profile websites, in order to draw attention to issues such as internet censorship”.

> “An excellent starting point is having an incident response plan in place; a formal, written document that is approved by senior management, providing a set of instructions for organisations to detect, respond to and recover from a cyber incident.

Anonymous Sudan launched DDoS attacks against countries such as Sweden, Denmark and the US in early 2022 that continued into this year, with the group announcing that it would target the US and European financial sector in mid-June. From the end of July, Kenyan organisations were under siege, and a number of businesses within the country such as banks, media, hospitals, universities and other companies were all reportedly targeted in a days-long DDoS offensive.

The effects of these attacks are far-reaching, says the report, numbering challenges such as service unavailability, loss of revenue, decreased productivity, remediation costs and reputational damage.

How, then, do African businesses take steps to mediate this type of attack, or at least minimise the damage wreaked by cybercriminals? The answer is to ensure that the right strategic steps are in place.

Setting up an incident response plan

An excellent starting point is having an incident response plan in place; a formal, written document that is approved by senior management, providing a set of instructions for organisations to detect, respond to and recover from a cyber incident.

Should an attack take place, the business would then consult its incident response plan and take the recommended steps.

For example, Datacentrix's incident response plan follows several stages:

1. The first, once the plan is invoked in the case of a cybersecurity incident, is to alert all responsible people within the business, including the governance and risk officer, senior management and executives.
2. The next step is to put together a team of security experts from the Datacentrix Security Operations Centre (SOC), which would encompass members from within different disciplines of cybersecurity.

3. Datacentrix would then open a 'war room', incorporating all its technical cybersecurity experts, who are tasked with investigating the attack, devising what needs to be done from a mitigation perspective, and carrying out the necessary measures.
4. All stakeholders would be kept up-to-date with progress during this process.

Ideally, an incident response plan should cater for all types of cyberattack, and whether it be ransomware or a malware attack, for example, the response should always remain the same – at least initially. This means that all members of the technical and operational teams are involved in the early stages, until it is decided how mitigation will be carried out. If different teams are assigned to manage different types of attack, the business runs the risk of losing sight of the bigger cybersecurity picture and could leave itself vulnerable to other types of incidents.

Proactivity is key

Datacentrix's advice is that organisations must not only have an incident response plan in place, but ensure that it is regularly put to the test. This could be carried out through attack simulations (penetration testing) to check for exploitable vulnerabilities, let's say, at least two to four times a year. These exercises will confirm that, as far as possible, all stakeholders and teams involved are ready for a real attack on the business.

In addition, companies must do frequent checks with their security engineering teams to confirm that they have the right security certifications in place.

Another essential exercise is making sure that the business offers ongoing cybersecurity training for end users. This is of paramount importance, considering that more than 80 percent of attacks are caused by human error.

You've been attacked, what next?

It's becoming less and less likely that African businesses will remain unscathed from cyberattacks, so it's important to look at how to recover in the event of an incident.

To begin with, the organisation must look at the type of incident experienced and see how it can then take more effective steps to secure its business systems from similar future attacks.

Again, the company should also look at more effective end user training, as well as raising awareness around its incident response plan with stakeholders, ascertaining what the plan means to the business and how it can be improved.

Businesses that do not have a dedicated internal security team should look for support from an established cybersecurity partner that offers Security Operation Centre (SOC) services.

An outsourced SOC delivers the benefits of immediate, 24x7 access to a team of cybersecurity experts as well as the latest advanced technologies, shared threat intelligence, scalability options, and also reduced operational costs.

In addition to the bouquet of powerful, proactive, multi-disciplined cybersecurity measures, an experienced cybersecurity partner will furthermore be able to assist with the establishment of a rock-solid incident response plan and regular simulations and testing scenarios.

> An outsourced SOC delivers the benefits of immediate, 24x7 access to a team of cybersecurity experts as well as the latest advanced technologies, shared threat intelligence, scalability options, and also reduced operational costs.

Brian Smith
Business Unit Manager, Datacentrix

For more information on Datacentrix's Security Services offering, visit https://www.datacentrix.co.za/security-services.html