+27(0)11 517 3000 nkonki.com hello@nkonki.com

Experience Ingenuity.

The Missing Elements in IT Security initiatives

In the recent months, reports of Information Technology (IT) security breaches have increased drastically and have resulted in data loss and in many other incidences, including financial and reputational loss as well.

Verizon publishes an annual Data Breach Investigations Report (DBIR) in which it details the 'who, what, where, when and how' of data breaches and cybersecurity incidents. A snapshot of the DBIR's executive summary paints an interesting picture: the public sector ranked 3rd as the most attacked and malware installed via emails as the most common attack vector.

Figure 1 below outlines a summary of the DBIR results.

Who are the victims?

24%
of breaches affected financial organisations.

15%
of breaches involved healthcare organisations.

12%
Public sector entities were the third most prevalent breach victim at 12%

15%
Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66%
of malware was installed via malicious email attachments.

73%
of breaches were financially motivated.

21%
of breaches were related to espionage.

27%
of breaches were discovered by third parties.

Figure 1. Verizon (2017)

nkonki

Registered Auditors | Accountants | Advisors

Interestingly, 88% of breaches outlined by Verizon in 2017 fell into nine (9) patterns that were identified as far back as 2014. These are:

- Crimeware (Ransomeware being the most common);
- Cyber-Espionage;
- Denial of Service;
- Insider and Privilege misuse;
- Physical theft and loss;
- Web Application attacks;
- Payment Card skimming;
- Point of Sale intrusion; and
- Miscellaneous errors.

Zooming in on the public sector, the most prevalent patterns that were exploited were:

- Cyber-Espionage, with 90 of the reported 113 breaches being from state-affiliated threat actors;
- Insider and Privilege Misuse; and
- Miscellaneous Errors that resulted in compromised security data.

Nation-State, Activist, Unaffiliated and Organised Crime threat actors all fall within 1.1% of the reported 113 breaches of Cyber Espionage.

It would be interesting to establish how many of the breaches actually related to the South African environment, but unfortunately, Verizon do not stratify in this manner.

South Africa, may be quick to dismiss the patterns noted in the DBIR report as only applicable to the first world, however, our status as a quasi-first world country means that we are just as susceptible as the United States, Brazil, India, Britain etc. when it comes to interest from threat actors. Verizon articulates clearly that South Africa contributed to their data and research report as outlined in Figure 2 below.

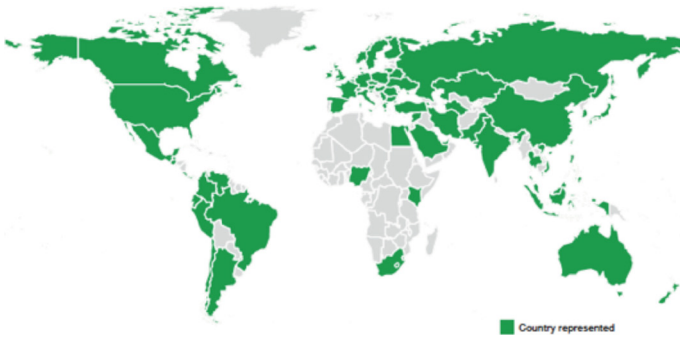

Figure 2: Verizon (2017)

Given Verizon's findings on the Public Sector and assuming it aligns to the South African context, what can this sector do to ensure that successful breaches are reduced?

The answer may lie in proposals from an established authority on Cyber-Security, i.e. Centre for Internet Security (CIS). This organization was founded in 2008 when it was created from a collaboration of the U.S government and the private sector security research organisations. In answering the question, "Where should I start when I want to improve my cyber defences and general IT Security posture?", CIS have developed a set of 20 controls that addresses most of the cyber security threats any organization will ever face. They further claim that by implementing what they call the "first 5 CIS controls" an organisation will have put in place an effective defence against the most prevalent forms of attack. The full scope of the suggested controls are outlined in Figure 3.

1	Inventory of authorised & unauthorised devices
2	Inventory of authorised & unauthorised Software
3	Secure configurations for hardware and software
4	Continuous vulnerability assessment & remediation
5	Controlled use of administrative privileges
6	Maintenance, monitoring, & analysis of audit logs
7	Email and web browser protections
8	Malware defenses
9	Limitation and control of network ports
10	Data recovery capability
11	Secure configurations for network devices
12	Boundary defense
13	Data protection
14	Controlled access based on the need to know
15	Wireless access control
16	Account monitoring and control
17	Security skills assessment and appropriate training to fill gaps
18	Application software security
19	Incident response and management
20	Penetration tests and red team exercises

Figure 3: CIS 20 Controls

These 20 controls simplify cyber-security efforts by cutting through the complexities of varied opinions, standards, trends, regulatory and compliance requirements. They have also been created in such a way that they align with best practice frameworks such as PCI, ISO, HIPAA (in the USA), COBIT etc. CIS created these controls using a global expert community in securing networks and they also taken and incorporated feedback from user communities. The first five (5) controls involve ensuring that:

- An organisation is aware of the inventory of authorised and unauthorised devices and software on its network(s);
- Hardware and software is securely configured including mobile devices, laptops, workstations, servers, networking devices etc.;
- Continuous or at least periodic vulnerability assessment and remediation; and
- Controlled use of Administrative Privileges.

A quick self-check of these controls in most State Owned Entities (SoE), National and Provincial Departments as well as Municipalities will reveal that none of these controls in place are in a matured manner. Perhaps only "Controlled use of Administrative Privileges" is something that is adequate but partially effective due to failure in monitoring key activities. It is our view that in most of the entities assessed, there have always been challenges with respect to 'how' to practically implement monitoring strategies.

As a firm with exposure to the Public Sector, any maturity assessment on these five (5) controls will outline the first four (4) as ineffective and the last one being partially effective. Such a picture should encourage the Public Sector to take Cyber Security seriously and at least perform a gap analysis based on these key controls and thereafter craft a remediation program that focuses on the first four (4) controls as a start.

To build a successful cyber-security program, the Public Sector will need to make high-level and transversal decisions to make these controls a standard part of the sector's cybersecurity efforts. Transversal efforts through National Government, permeating to Provincial and Municipal Structures will need to be established to ensure that program managers are empowered to implement these controls. The legislated IT Strategies should include a cybersecurity component that will allow three to five years plans to be adopted to implement the cybersecurity practices that are not already part of an entity's current posture. This should include amending security policies to include CIS Controls, encouraging internal and external assurance providers to use CIS controls as part of benchmarking efforts and educating the workforce on the entity's cybersecurity goals as well as encouraging the workforce to be part of the efforts.

Contact us

For more information on "The Missing Elements in IT Security initiatives" contact Nkonki on: +27 11 517 3000

References::
Verizon, Data Breach Investigations Report (DBIR), 2017, Retrieved from:
- http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_execsummary_en_xg.pdf
- CIS, Implementation Guide for SMEs, https://www.cisecurity.org/white-papers/cis-controls-sme-guide/

Contact Details

Johannesburg - Head Office

Physical Address:
Nkonki House 1
1 Simba Road
Sunninghill
Johannesburg

Durban Office

Physical Address:
131 Jan Hofmeryer Road
Westville
3629
Durban

Stanger

Physical Address:
84 Balcomb Street
Stanger
4449

Pretoria Office

Physical Address:
638 Jacqueline Drive
Garsfontein East
Pretoria
0081

Bloemfontein

Physical Address:
95B Kellner Street
Westdene
Bloemfontein
9301

Cape Town Office

Physical Address:
1st floor, Block A, Regent Square
Kenilworth
7708

Alberton Office

Physical Address:
DVM Office Park, 1st Floor
16 Kingfisher Crescent
Meyersdal
Gauteng

Northwest

Physical Address:
48 Proctor Avenue
Golf View
Mafikeng
2745

Port Elizabeth

Physical Address:
3 Redheart Crescent
WaveCrest
Jeffreys Bay
6330

Jeffreys Bay

Physical Address:
3 Redheart Crescent
WaveCrest
Jeffreys Bay
6330