**NATIONAL ASSEMBLY**

**QUESTION FOR WRITTEN REPLY**

**PARLIAMENTARY QUESTION NO: 1149**

**DATE OF QUESTION: 25 MARCH 2022**

**DATE OF SUBMISSION: 08 APRIL 2022**

**Adv G Breytenbach (DA) to ask the Minister of Justice and Correctional Services:**

1. Following the disastrous hacking and ransomware attack on the information and communications technology infrastructure of his department in 2021, what (a)(i) steps have been taken and (ii) preventative measures have been put in place to ensure that this does not happen again;
2. What measures have been put in place to ensure that the systems of the (a) Office of the Master of the High Court and (b) High Court function independently?

**NW1402E**

**REPLY:**

1. The Department of Justice and Constitutional Development (DoJ&CD) has implemented a wide range of security measures within its information processing environment, intended to prevent any unauthorized access to and/or use of sensitive information and ensure that the confidentiality, integrity and availability of personal information remain protected. These security measures are categorized into two (2) groups as follows:
2. Managerial controls, including a set of approved, published and implemented information security policies, standards, procedures and guidelines. Awareness of the existing information security policies and cybersecurity risks within our information processing environment is proactively and regularly being promoted amongst DoJ&CD’s users to ensure positive security behaviors and adherence to prescribed rules.
3. Technical Controls – In addition to the native security features provided by our systems and platforms, we have deployed a set of automated security tools and processes to improve our defensive capabilities and safeguard our ICT infrastructure and systems. These technical tools enable us to effectively restrict and control access to our ICT systems, applications and services, manage vulnerabilities, proactively monitor, protect and respond to security threats and incidents. We have also deployed disaster recovery capabilities to ensure continued availability of business-critical information in case of any adverse event impacting DoJ&CD’s services. Technologies that are currently implemented include:
4. **Antivirus –** Endpoint (PCs) Antivirus Software. All endpoint devices were equipped with Antivirus software which offers advanced automated threat detection and response against an ever-growing variety of threats and malware.
5. **Advanced Threat Protection** – A limited number of critical servers have protection against attacks, advanced threats and ransomware, giving the Departments the power to detect, analyze and respond today’s stealthy attaches in real time.
6. **Network Discovery and Analysis –** A limited number of critical services have advanced tools installed that provides 360 degrees of visibility by monitoring and reporting on all network ports network traffic. This detects targeted attacks designed to evade standard security solutions.
7. **Mail Security Gateway –** providing Integrated-tiered spam prevention and anti-phishing spyware. The appliance provides a comprehensive gateway email security.
8. **Web Security Gateway –** Provide a proactive web traffic detection and blocking services based on reputation services.
9. **Firewalls –** Network security appliance that monitors and controls incoming and outgoing network traffic based on predetermined security rules. This device typically establishes a barrier between a trusted network and untrusted networks such as the internet. The firewall provides protection against outside cyber-attackers by shielding the Department’s computers or network from malicious or unnecessary network traffic.
10. **MIMECAST –** Provides theDepartment with email security services. It is used to protect the Department’s email system, ensure access and simplify the tasks of managing emails system.
11. **Security Information and Event Management (SIEM) –** A Software solution that aggregates and analyzes activity from many different resources across your entire IT Infrastructure. SIEM collects security data from network devices, servers, domain controllers, and may more log sources. SIEM provides real-time analysis of security alerts generated by applications and network hardware.
12. **Proxies –** This solution offers the Department reverse proxy services. A reverse proxy ultimately forwards user/web browser requests to the web servers. However, the reverse proxy server protects the web server’s identity. It helps increase performance, security and reliability.
13. **Vulnerability Scan Tools –** These tools were deployed in the environment to scan and report on a quarterly basis the vulnerability levels of the Department in terms of missing patches.
14. **Virtual Private Network Technology –** This tool grants complete access to the Department’s Local Area Network to authorized users via encrypted secure tunnels.
15. **User awareness and training tools –** These tools allow the Department to provide target security awareness messages to end users. It also allows for simulated attacks and end user training in the event where awareness is lacking. Post the breach, this tool was deployed to 2000 users in the Headquarters, with plans to roll it out to all users in this financial year.
16. In addition to the already implemented security tools, the Department has, post the ransomware, enabled the following additional security measures:
17. **Zero Trust Network Tool –** The Zero Trust Network Access Tool will help the Department to provide secure remote user access to applications and services based on defined access control policies, the tool defaults to deny, providing only the access to services the users has been explicitly granted. With this Zero Trust Network Tool, access is established after the user has been authenticated to the tool first. The tool then provisions access to the application on the user’s behalf through a secure, encrypted tunnel. This provides an added layer of protection for the Department’s applications and services by shielding otherwise publicly visible Internet Protocol (IP) addresses. With this solution, users will only see applications that they have access to. This tool is to replace the current VPN tools which grant complete access to all applications.
18. The Department also implemented a tiered administrative model on the active directory and that will help the Department to better secure its ICT environments. The model defines three (3) tiers that create buffer zones to separate administration of high-risk PCs and valuable assets like domain controllers.
19. We have also reviewed and/or enhanced our security policies on all our security appliances to safeguard against future security attacks.
20. Going forward, the following technologies are to be implemented to further enhance the security of the ICT environment:
21. Cyber Security Operations Centre (CSOC) will be implemented in the 2022/23 financial year.

CSOC is a centralize function within an organization employing people, processes and technology to continuously monitor and improve an organization’s security posture while preventing, detecting, analyzing and responding to cybersecurity incidents. CSOC will act like the hub or central command post, taking in telemetry from across the Department’s IT infrastructure, including its networks, devices, appliances, and information stores wherever those assets reside. The proliferation of an advanced threat places a premium on collecting content from diverse sources. Essentially, the CSOC will be the correlation point for event logged within the Department. This will be implemented by way of a hybrid model using existing tools aggregated on the one platform.

1. External Penetration Testing.

Discussions and planning had already commenced with some of the industry partners in terms of providing a comprehensive external penetration testing, with the aim of identifying any gaps in our security environment. This process is expected to be finalized by the middle of the year, and be completed annually going forward.

1. Where the Master of the High Court and the High Court share the same building, each operates independently as the Master’s Office falls within the ambit of the DoJ&CD and runs on the DoJ&CD Virtual Private Network (VPN), whereas the High Court falls under the ambit of the Office of the Chief Justice (OCJ) and runs on the OCJ VPN.