Dandemutande

Cyber Security Portfolio

Table of Contents

Introduction

In this current world of information and technology with various complex hazards and malware, it is critical that the company's IT systems are protected with more efficient security measures. Dandemutande is offering various ICT security solutions with the necessary hardware in order to protect companies and their Computer Network Systems from intruders, hackers, fight against malware and control the employees' access in the company most valuable asset which is DATA.

Product listing

- Network Security Firewalls
- Endpoint / Antivirus
- Email Security
- Data Encryption
- Virtual Private Networks (VPNs)
- Physical Security
  - CCTV
    - Home Security
    - Enterprise Security
  - Access control
    - Biometrics
    - RFID Tags
- Vulnerability Assessments and Penetration testing (VAPT)

1. Network Security Firewalls

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) to block malicious traffic like viruses and hackers.

1.2 Dandemutandes Physical and Virtual firewall security solution.

- Sophos firewalls
- Fortinet firewalls
- Linux firewalls
- Mikrotik firewalls
- Cisco firewalls
- Cisco Umbrella Firewalls
- Microsoft firewalls etc.

1.2 Benefits of a Firewall

- Monitors Traffic - monitors all the traffic entering or leaving your Private computer network.
- Monitors and blocks intrusions – as Trojan horses and other malicious Software's
- Stops Hackers - keeps hackers out of your network
- Enforcing usage policy within the organisation by defining what can and cannot be done on an office network.
- Provides usage stats in detail
- Stops Hackers. Having a firewall keeps hackers out of your network.
- Stops Keyloggers. Having firewall security will reduce the risk of keyloggers monitoring you.
-

2.Endpoint Security

Endpoint security refers to securing endpoints, or end-user devices like desktops, laptops, and mobile devices. Endpoints serve as points of access to an enterprise network and create points of entry that can be exploited by malicious actors.

Endpoint security software protects these points of entry from risky activity and/or malicious attack. When companies can ensure endpoint compliance with data security standards, they can maintain greater control over the growing number and type of access points to the network.

"Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage

2.1 Dandemutandes Endpoint/Antivirus security solutions
- Sophos endpoint
- ESET endpoint
- Webroot
- Norton endpoint etc.
- MacAfee endpoint

2.3 Importance of Endpoint Security:
- Endpoint security aims to adequately secure every endpoint connecting to a network to block access attempts and other risky activity at these points of entry.
- Mitigate attacks before they happen.
- Prevents Data theft.
- Protects computing resources from processing unproductive malicious activities.

3. Email Security

Dandemutande's Email security measures are used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts. Some of these emails are called, Spam, Junk email or unsolicited messages.

3.1 Email Security Solutions at hand are: -

1. **Spam Shield-** this is a user configurable suite of tools to reduce junk email. Spam-Shield blocks over 99.9% of spam, viruses, malware, and other email threats. We provide advanced email security for your business without making it complicated. Unsolicited emails, phishing attempts, spoofing and illicit content are just some of the categories of unwanted email that Spam-Shield blocks.

2. **Sophos Email Protection -** Sophos Email Appliance provides advanced protection against spam and phishing attacks, Sophos Time-of-Click protection blocks malicious email URLs to protect against stealthy, delayed, spear phishing attacks – securing every URL, in every email.

3. **Microsoft Advanced Threat Protection -** Microsoft Office 365 Advanced Threat Protection (ATP) is a cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection, and includes features to safeguard your organization from harmful links in real time

3.2 Benefits of Email Security

- Ensured confidentiality
- Secure DNS Filtering. Control access to malicious websites.
- Secure Web Gateway. Defend from any internet-based threats.
- Secure Email Gateway. Stop email threats before it enters your inbox.
- Data Loss Prevention. Preserve and protect your sensitive data.

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data

4. Data Encryption

Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission.

4.1 Partners

1. **IBM Guardium Data Encryption.**
   - Protect your file and database data from misuse and help comply with industry and Government regulations with this suite of integrated encryption products

2. **Check Point Full Disk Encryption Software Blade**
   - Provides automatic security for all information on endpoint hard drives, including user data, operating system files and temporary and erased files

3. **ESET DESlock**
   - Data encryption for files on hard drives, portable devices and sent via email

4. **Dell Encryption Enterprise**
   - Provides software-based, data-centric encryption that protects all data types on multiple endpoints and operating systems. Dell Encryption Enterprise also integrates with existing authentication processes, including Windows password, RSA, fingerprint, and Smart Card.

5. **McAfee Complete Data Protection**.
   - Drive encryption, file, folder, and Cloud storage encryption

6. **Sophos Safeguard.**
   - Encrypts content as soon as it is created. The encryption is always on, allowing for seamless and secure collaboration. This method promotes secure collaboration everywhere, working across device and platforms without compromising security and preventing accidental data leakage.
   -

4.2 Benefits of Data Encryption

- Complete Data Protection of data in transit or in storage
- Security Across Multiple Devices.
- Enables you to move Data Securely.
- Maintained Data Integrity.
- Ensure Compliance.

5. Virtual Private Networks

Virtual Private Network (VPNs), are a solution that allows the establishment of a safe and encrypted point-to-point connection to the company's internal network through an unsafe channel. The VPN connection ensures safe data communication for users outside

the office and allows the connection of several office networks into a joint network to access office resources.

5.1 List of VPNs Dandemutande is providing: -

- Remote Access VPN.
- Site – to – Site VPN.
- Internet Protocol Security or IPsec.
- Layer 2 Tunnelling Protocol (L2TP).
- Point – to – Point Tunnelling Protocol (PPTP).
- Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
- OpenVPN.
- Secure Shell (SSH)

5.2 Benefits of VPNs

- A VPN hides your Online identity.
- VPNs help you bypass Geo-Blocks.
- VPN services secure your Online connections.
- A VPN can prevent bandwidth throttling.
- VPNs can bypass Firewalls.
- VPNs offer secure Torrenting.

6. Closed-Circuit Television – CCTV

Closed-circuit television (CCTV), also known as video surveillance, is generally used for monitoring continually or to monitor one happening.

6.1 Home Security

With the continuous criminal activities like house break-ins, burglaries and tempering in the world today, Dandemutande takes pride in offering home surveillance system to safeguard homes and your families.

Dandemutande has two home security solutions, which are: -
1. Ring security surveillance system
2. SimpliSafe home surveillance system

The Ring and SimpliSafe solutions give you and easy installation and peace-of-mind solution for your home. They come as a standard packaged set and can be customised depending on the area of security concern to be covered.

6.2 Enterprise Security

Depending on the size of premises to be monitored, Dandemutande's Enterprise security solution is upon a survey by our CCTV engineers.
Dandemutande's Home and Enterprise Security is/can be coupled up with Smart, Advanced video Analytics.

What is Video Analytics?

Video Analytics Suite provides a powerful enhancement to the world-class, feature rich CaVideo Surveillance Management software, and significantly enhances the value of any CCTV surveillance installation. It goes beyond surveillance to offer the most sophisticated and fully integrated infrastructure and security management system that delivers maximum return on surveillance investment.

Seamless integration, easy installation and exceptional ease-of-use have made it the preferred surveillance software solution for the global retail, banking, mining, education, residential, commercial, healthcare, transport, logistics and city surveillance sectors.

The Video Analytics Suite offers: -

- Presence Detection
- Enter/Exit Area
- Human head count

- Line-Crossing Analytics
- Motion Detection
- Time or Stop in Area
- Direction
- Speed
- Loitering
- Object Detection and Count
- Appear/Disappear
- Queue Length Analysis
- License Plate Recognition

Brands and Models provided: -

- Hikvision
- Dahua
- Samsung
- Ubiquiti
- Axis
- Bosh

7. Access Control Systems

7.1 Biometric

Biometrics are physical or behavioural human characteristics to that can be used to digitally identify a person to grant access to systems, devices, or data. This can be **fingerprint, facial** recognition and more. Today, Biometric Access Control system is ranked one of the best and most secured and accurate authentication systems amongst the other access control devices.

Brands/Models on offer: -
- Dahua
- ZK software
- Impro

7.2 RFID Tag system

The Tag system uses RFID in Access Control, using radio-frequency electromagnetic fields to identify people of objects without making physical contact. The typical RFID-based controlled access solution consists of tags that contain unique identification data capable of granting or denying access to individuals.

Brands/Models on offer: -
- Dahua
- ZK software
- Impro

8. VEHICLE TRACKING

Dandemutande has the surveillance and tracking of vehicles as a security product. Knowing the whereabouts of your personal vehicle and/or company fleet when there is a theft or general monitoring policy to be enforced is of paramount importance.

Our vehicle tracking system has the list of features: -

8.1 Dashboard

- Our dashboard has been designed to give you all the critical data you require in just a few clicks. You can run any report or map for a single vehicle or your entire fleet. With the Dandemutande dashboard at your fingertips you will have complete access to your fleet and start to experience the benefits of being in total control of your business

8.2 Alerts

- From protecting your business and reputation to the safety of your workforce our customised alerts (via email or SMS to an unlimited number of recipients) allow you unprecedented access and information to the critical factors that can impact your business.
  - o Speeding and Excessive Idling Alerts - Help you to reduce fuel costs, maintenance costs and cut carbon emissions.
  - o Geo-Fence Alerts - Predefine Geofence locations such as your premises, your client's premises and rest stops and receive alerts when vehicles enter or exit Geo-Fences.
  - o Fatigue Management Alerts - Receive alerts when drivers breach regulated fatigue rest periods.
  - o Rollover Alert - Receive alerts when vehicle has rolled over
  - o Harsh Braking Alerts - Receive alerts when vehicle brakes have been excessively applied.
  - o Theft Alert – Receive alerts when your vehicle has been moved when the ignition has not been turned on in the correct manner or is being towed without an ignition on.

8.3 Reporting

- The ability to receive data across your fleet in real-time, enables you to adapt to any adverse conditions and always remain one step ahead.
- This not only makes your job a lot easier, it also allows you to have an edge on the competition.
- The Dandemutande fleet management system provides customised and robust on-demand reporting that ensures you are in the driving seat and have exactly the information you need when you want it. This improves efficiency, reduces operating and maintenance costs and gives you total control over your mobile assets.
- The Dandemutande fleet management system allows you to locate your vehicles on a map in seconds and is incredibly easy to use. A full reporting suite lets you download and review reports in real-time, as well as schedule reports to be automatically generated and sent to any email address.
- Reports Include:
  - All Positions Report
  - Location History Report
  - Demurrage Report
  - Excess Idle Report
  - Driver Scorecard Report
  - Vehicle Scorecard Report
  - Service Due Report
  - Fatigue Management Report
  - Speeding Report
  - Utilisation Report
  - Trip Report (By individual, vehicle, or time)
  - Vehicle Work Summary Report
  - Vehicle History Report
  - Alerts Report (Speeding, Geofence, Fatigue, Excess idle etc)

8.4 Vehicle History

- The historical data of your vehicles can become valuable information to a fleet manager or services company.
- The ability to review vehicle utilisation, daily usage, and route selection aids in calculating better efficiencies and savings. This is a powerful tool in making informed business decisions and to plan accordingly for the future.

8.5 Geo-Fencing

- The ability to set virtual perimeters around an area allows a vehicle or expensive plant machinery to be monitored on a regular basis.
- Alerts are very easy to set up and enable you to be aware of any activity outside of the Geo-Fencing.
- Designed to meet your needs and offer peace of mind by improving security, operational control, and proof of work.

8.6 SOS Alerts

- Dash mounted SOS Switches and personal pendant mounted SOS buttons complete the remote worker safety solution.
- The Dandemutande device in conjunction with SOS buttons allow remote staff to send an SOS signal via email and/or SMS to several recipients in the event of an accident, breakdown, or any dangerous situation.

8.7 Driver Identification

- Driver ID couples detailed information about a vehicles activity with specific driver activity letting you manage timesheets easily and make sure the right driver is carrying out the work you intended. With driver ID you can identify and reward efficient and safe drivers as well as identify development opportunities in others. Dandemutande's driver ID helps you manage your resources and maintain your duty of care by linking records on driving licenses that help ensure drivers only drive vehicles they're qualified for. And alerts can let you know when unidentified or unqualified drivers are moving your vehicles for extra peace of mind.

9. Vulnerability Assessments and Penetration testing (VAPT)

What is VAPT?

Vulnerability Assessment and Penetration Testing (VAPT) are two types of vulnerability testing. Also called Pen-test. It is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations, or risky end-user behaviour. Such assessments are also useful in validating the needed achievement of defensive mechanisms, as well as, end-user adaption to security policies. Pen-tests are subjected to internal and external vulnerabilities.

9.1 Types of Penetration Testing

- **White-box testing**: which provides background and system information from the client.
- **Black-box testing**: which provides only basic or no information except the company name from the client.
- **Grey-box testing** is a combination of the two (where limited knowledge of the target is shared with the auditor).

9.2 Source/supplier/Partners
- Bytes
- Baker Tilly
- Metro Access
- Ambrose

9.3 Penetration Testing Benefits:

- Validate internal and/or external security controls, including protections around customer's network and systems.
- Manual testing that simulates current threats, including pivoting and post exploitation.
- Satisfy compliance needs i.e. from Audit.
- Confidence in the assessment knowing that the latest threat intelligence and tactics from Dandemutande were utilized.
- Tests users in conjunction with your external and internal networks.
- Simulates a common real-world threat.
- Tests your response and detection capabilities.

10. PARTNERSHIPS

11. FIREWALL COMPARISONS

Features	Sophos	Fortinet	Cisco
Security Performance	97.82%	99.71%	95.5%
Performance		SD-WAN, advanced routing, and WAN optimization capabilities	provide DDoS protection and multi-factor authentication.
Value		Very Good	traffic inspection and the Firepower engine
Implementation	Configuration troubleshooting through color-coded, live firewall log.	Easy to manage	
Support		Lack direct vendor support	
Cloud features		Support for multiple virtualization and cloud environments.	Offer virtual appliances and cloud functionality.
Pricing		Reasonable and least expensive	Expensive

.