2020

AN OVERVIEW OF CYBERSECURITY

BRIGHTRED RESOURCING LIMITED

MARCH 2020

AN OVERVIEW OF CYBERSECURITY

As the world moved into a digital era, security threats turned digital too. Gone are the days when businesses simply installed firewalls and antivirus solutions to secure their networks. With the rapid proliferation of integrated technologies such as cloud computing, Internet of Things (IoT), Bring-your-own-Device (BYOD), Artificial Intelligence solutions etc., business networks are no longer a private entity. As such, businesses are now required to implement a comprehensive cybersecurity environment that can protect all touch points of the network across the infrastructure, regardless of their nature and size.

Cybersecurity is an umbrella term that encompasses all the tools, technologies, approaches, best practices and solutions implemented in securing a digital infrastructure.

Data breaches haven't started with digitalisation of information. They happened in the non-digital era too. However, in the digital era, the cost of a data breach is massive. For instance, the data breach incident of Yahoo in 2013-2014 affected 3 billion users. Similarly, First American Financial Corp network was hacked in 2019, affecting 885 million records.

According to the Q3 Data Breach report from Risk Based Security, **5,183** data breaches were reported in 2019 affecting 7,995 million records which is 33.3% higher compared to its 2018 report. When it comes to breach types in 2019, hacking leads the list with 3,917 breaches followed by 341 skimming cases. While 4,527 breaches were caused by outsiders, 567 cases were caused by insiders in 2019. Emails and passwords were the most hacked data types accounting for 65.1% and 59.1% of breaches respectively. When it comes to sectors, healthcare stands at the top with 343 breaches in 2019 followed by retail and public sector with 307 and 264 cases respectively.

In the UK, 111 data breaches were recorded in October 2019 accounting for 421 million records affected, as reported by IT Governance, UK.

TYPES OF DATA BREACHES

While data breaches happen through multiple procedures, here are the most common types of data breaches:

a) **Distributed Denial of Service (DDoS):** In this method, hackers attack a website or a network by overwhelming it with virtual traffic so that all website resources are exhausted. When it is done at a massive scale, it is called DDoS. As such, the network cannot handle the traffic and becomes inaccessible. A notable example is the DDoS attack on DNS site Dyn in October 2016

wherein multiple websites powered by it such as PayPal, Visa, CNN, Airbnb were brought down.

b) **Ransomware:** In this method, hackers access the network and encrypt data and files on the network. Then they charge a ransom price to decrypt the data. Upon paying the ransom amount, the files are decrypted. A notable example is WannaCry ransomware that affected more than 200,000 computers in 150 countries in May 2017. In the UK the National Health Services (NHS) was the most affected organisation where 70,000 computers were infected with this ransomware.

c) **Phishing:** Is a technique used by hackers to gather information from a person. They send emails that seems to be from legitimate

institutions but are not. When the user clicks any link in the email, it redirects them to their website to collect crucial information from the person. Voice calls, social media and 'chats' are also used by hackers to gather the required information.

d) **Malware:** An umbrella term that comprises multiple elements such as viruses, trojans, spyware, ransomware, adware, botnets etc. Malware is a software code written by hackers to steal data, damage computing

devices and disrupt networks.

TYPES OF CYBERSECURITY SOLUTIONS

Cybersecurity is an umbrella term that comprises of multiple security solutions implemented by organisations. Here is a list of common types of cybersecurity solutions.

APPLICATION SECURITY

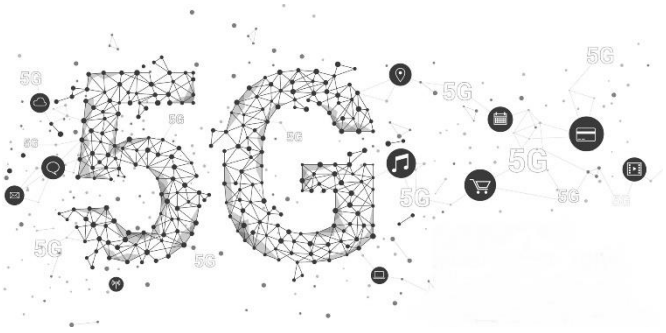
Application Security is a framework of security policies, practices and tools for identifying, fixing and protecting an application throughout its lifecycle. It includes testing tools that test the application and shielding tools that shield and protect the application after deployment. While application security deals with securing an application, it involves other security aspects such as endpoint security, mobile security, network security, cloud security, data security etc. Businesses use various methods to secure applications such as Authorisation, Authentication, Encryption, Logging, security testing etc. QA teams use Static Application

Security Testing (SAST) to scan source files and Dynamic Application Security Testing (DAST) to test running apps in a simulated environment. Similarly, there are different methods to secure web apps, mobiles apps and cloud apps. In DevOps where continuous development and deployment are in place, businesses are now integrating application security into their development environment.

IBM Security AppScan, Checkmarx, MicroFocus Fortify, Synopsys Black Duck, Veracode App Security Platform etc. are some of the leading application security tools available in the market. Open Web Application Security Platform (OWASP) is an open-source application security tool that helps open source developers in securing their application development environments.

NETWORK SECURITY

Network Security is a framework of technologies, policies and practices to assess and protect the integrity of a network and the data managed across the network. It involves the arrangement of software and hardware tools in a multi-layer defence system to protect network infrastructure from unauthorised and malicious access. Network security tools detect and react to unauthorised access and protect the network. Antivirus, Firewall protection, network access control, virtual private networks, network segmentation, network access control (NAC), behavioural analytics, intrusion prevention system etc. are some of the techniques used by network administrators to secure a network.



A normal network security system handles three important aspects of the network namely Physical network security, Technical network security and Administrative network security. While physical network security is about physical controls such as biometrics, locks etc., technical network security secures data. The administrative network security comprises of user access control policies.

When it comes to network security tools, there are hundreds of tools that serve in different categories. Veracode, OpenVAS, OSSEC, Nikto, Cisco etc. vendors for some of the popular network security products.

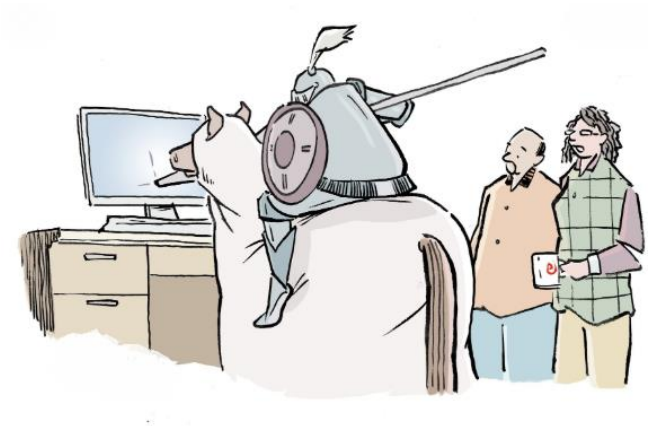
IDENTITY AND ACCESS MANAGEMENT

IAM is a process of defining and managing digital identities for individual users on a network. It comprises of all technologies, policies and processes used for providing role-based access to users. The IAM security framework enables businesses to control who accesses what type of information on the network. Single sign-on, multi-factor authentication, Privileged access management (PAM) etc; are some of the techniques used in IAM. Different technologies

used in IAM include Identity Management and Governance (IMG), Identity as a Service (IDaaS), Identity Analytics (IA), API Security Solutions, Customer Identity and Access Management (CIAM) solutions, Risk-based Authentication (RBA) etc.

Microsoft and AWS offer hybrid IAM solutions. Similarly, Centrify and Okta are offering cloud-based Identity as a service (IDaaS).

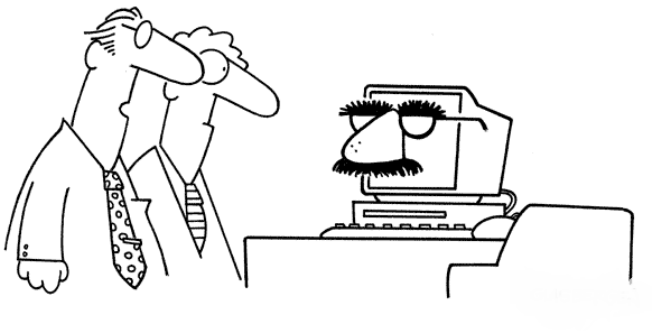
ENDPOINT SECURITY



Endpoint security comprises of all the policies and procedures used to protect endpoint devices such as mobiles, laptops and computer devices that act as an access point to a network. With BYOD networks, employees now access company resources from home or any other location. As such, endpoint security has now become critical for businesses of all sizes. Some of the functionality in endpoint security include application whitelisting, data classification, data loss prevention, network access control, privileged user control etc.

When it comes to endpoint security, all security solutions organisations offer endpoint security. Some of the popular ones are Comodo, Bitdefender, F-Secure, FireEye, ESET, Kaspersky, McAfee, Palo Alto Networks, Microsoft Endpoint Security, Sophos, etc.

DATA SECURITY



"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

Data security or information security defines the policies, standards and technologies implemented to safeguard data from unauthorised access. The primal focus is on the confidentiality, integrity and availability of data. It also involves protecting data from getting corrupt. Encryption, decryption, data masking, data erasure, data resilience, backups and disaster recovery programs are some of the methods used in data security. While authentication procedures are implemented for data access, compliance is also prioritised for highly regulated sectors that deal with health records, financial transactions etc. With real-time alerts, risk assessments and auditing, businesses can mitigate data breaches. In addition, the purging of data is also carried out on a regular basis.

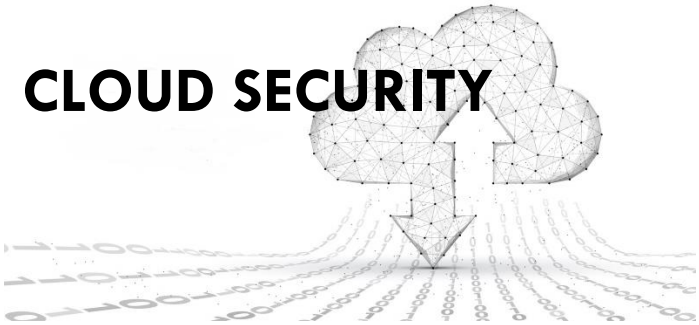
A few notable Data Center security tools are Cisco ACI, Symantec Data Center Security, Trend Micro Deep Security, Junos Space Security, FortiGate, HashiCorp Vault etc. When it comes to Data-Centric tools, Aptible, Stealth Audit Management, Netwrix Auditor, Arcserve UDP, Egnyte etc.

MOBILE SECURITY

Though mobile security falls into other security categories such as endpoint security, data security etc., it is specific to mobile devices such as smart phones, tablets, laptops etc. It is also referred as wireless security. As businesses implement BYOD and IT consumerisation via wireless networks the data on each mobile device has to be protected. Lost or stolen devices are a key concern for system administrators as they make networks vulnerable. Data leakage is another challenge. As such, each mobile device should be secured whilst compliance is also met. Companies either limit access to mobile devices or use additional programs to monitor and manage devices.

Microsoft Intune, Citrix XenMobile, IBM MaaS360, SOTI MobiControl, VMware AirWatch Manage Engine MDM Plus are some of the popular mobile security solutions.

CLOUD SECURITY



Cloud security uses policy-based technologies and controls implementation to protect, data, systems and networks in a cloud-based infrastructure. While cloud security is similar to on-premise security in many ways, the primal focus is on access, owing to its highly connected networks. Regular cloud security methods include but not limited to implementing strong IAM credentials, secure APIs, securing data, mitigating insider threats and account hijacking etc. Some of the cloud security tools available in the market are Skyhigh Networks, SilverSky, Okta, Bitglass, CipherCloud, AppRiver and Zscaler.

DISASTER RECOVERY PLAN

Disaster Recovery (DR) plan is sometimes called a Business Continuity Plan. However, a DR plan is actually a part of a business continuity plan. A DR plan is a security policy that defines keeping business critical functions running after a disaster. Whether natural or cyber-attacks, regardless of the type of disaster, businesses should be able to keep important functions up and running. DR plans include detecting an event, preventing an event and taking corrective measures. Having robust backup is the key here.

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are the two important aspects of a DR plan. While RPO talks about the files that should be recovered, RTO talks about the time for a recovery.

Some of the popular DR tools are Microsoft Azure Site Recovery, Carbonite Server Backup, Arcserve UDP Cloud Direct, Crashplan and Zerto.

DATABASE SECURITY

As the name speaks, database security is a set of security policies and procedures implemented by an

organisation to protect database management systems. It also includes protecting the data managed by the DBMS. Configuration of the DBMS is the key here. The next thing is to provide role-based access to authorised users. Auditing the databases, taking backups, encryption, decryption, masking, application security, system hardening, are some of the tasks involved in this framework. Similarly, using firewalls and virtual private networks are also included. Best practise is to isolate sensitive databases. Similarly, masking data for testing tasks is a good idea. MSSQL DataMask is a good tool to mask live data in sample databases. Remaining compliant with regulations such as GDPR is important too.

IBM Guardium, Mentis Suite, HexaTier, Oracle ADVF, Thales are some of the popular tools available in the market for database security.

THE STATE OF THE CYBERSECURITY MARKET

The cybersecurity market is on the rise. According to Allied Market Research, the global cybersecurity market earned a revenue of $104.60 billion in 2017. This value is expected to touch $258.99 billion by 2025. Similarly, MarketsandMarkets reports that the cybersecurity market was valued at $152.71 billion in 2018. This value is expected to reach $248.6 billion by 2023. Europe is the second rapid growths market for cybersecurity solutions as business are required to comply with GDPR regulations.

There are around 800 cybersecurity companies working in the UK. According to Great Gov UK, the UK cybersecurity market earned a revenue of £3.87 billion in 2018. The UK government's investment in cybersecurity solutions was £1.9 billion. The Banking, Financial Services and Insurance segment (BFSI) holds the major share in this market.

The Bottom Line

Cybersecurity is a special segment that cannot be taken lightly. A small error by an employee can run into huge revenue losses for an organisation. In addition, compliance issues add up to the damage. As such, organisations have to recruit the best professionals in this area. This is where Brightred comes to the rescue.

As a leading provider of specialist recruitment solutions, Brightred offers highly experienced and talented cybersecurity professionals for organisations of all sizes.

Call us right now to secure your Technology Estate

☎ 0203 8000 555

www.brightred.com