FREEDOMTECH SOLUTIONS

+44 (0) 0203 917 1777
sales@freedomtech.solutions
www.freedomtech.solutions

TECHNOLOGY SECURITY

EVERY ORGANISATION IS A POTENTIAL VICTIM.

In cybersecurity terms, we understand thatrisk is the potential for a threat (a person or thing that is likely to cause damage) to exploit a vulnerability (a flaw, feature or user error) that may result in some form of negative impact for your business.

Before investing in defences, we see many organisations often want concrete evidence that they not will be targeted by specific threats.

Unfortunately, in cyberspace, it is often difficult to provide an accurate assessment of the threats that specific organisations will encounter. However, we are aware that every organisation is a potential victim.

All organisations have something of value that is worth something to others. If you openly demonstrate weaknesses in your approach to cybersecurity by failing to do the basics, you WILL experience some form of a cyber attack. As part of your risk management processes, you should be assessing whether you are likely to be the victim of a targeted or un-targeted attack; every organisation connected to the Internet should assume they will be a victim of the latter. Either way, you should implement basic security controls consistently across your organisation, and where you may be specifically targeted, ensure you have a more in-depth & holistic approach to cyber security.

FREEDOMTECH SOLUTIONS

+44 (0) 0203 917 1777
sales@freedomtech.solutions
www.freedomtech.solutions

TECHNOLOGY SECURITY

SECURE YOUR BUSINESS

Freedomtech are working hard to help businesses better understand their vulnerabilities and how best to mitigate these threats, not just from outside infiltrators but from within the network itself - whether that be accidentally injected viruses via USB or email or targeted attacks from malicious staff.

Freedomtech in line with The National Cyber Security Centre (part of GCHQ) recommendation, suggest the following **five steps to help secure your business** from Cyberthreats:

- Secure your Internet connection
- Secure your devices and software
- Control access to your data and services
- Protect from viruses and other malware
- Keep your devices and software up to date

ENTERPRISE CLOUD BACKUP

Although no business can ever fully protect itself from vulnerabilities and threats, we see that there are many ways to take steps in fighting the ever-changing barrage of cyberattacks.

In order to assist your business in the fight for security, compliance and protection, Freedomtech has put together a suite of off the shelf and bespoke security services developed inhouse and through partners which creates an envelope of layers making it harder for perpetrators to gain access to your network, assets and data.

National Cyber Security Centre
a part of GCHQ

FREEDOMTECH SOLUTIONS

+44 (0) 0203 917 1777
sales@freedomtech.solutions
www.freedomtech.solutions

TECHNOLOGY SECURITY - SECURITY LAYER

INTELLIGENT NETWORKS AND FIREWALLS

Next-Generation Firewalls which include Application Visibility and Control, NGIPS, Advanced Malware Protection, URL filtering, Intrusion detection and DDoS mitigation.

NETWORK VISIBILITY

Use machine learning and AI algorithms to detect and respond to cyber-threats across diverse environments, including cloud, virtualised networks and IoT. This technology is self-learning in identifying threats in real time.

SECURE YOUR DATA

Freedomtech's Managed File Transfer (MFT) platform allows data to be transferred in a controlled, secure fashion, both inside and outside your organisation, between systems and/or users. Files are transferred more quickly and securely, enhancing productivity and providing visibility of transfers. Our service extends into email security using encryption and end to end scanning & validation.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Deploy a managed detection and response service that combines security information and event management (SIEM) technology with dedicated security experts that offer **24/7 network monitoring and investigation** of your organisation's network traffic. Cyber Security Operations Centre (CSOC) analysts and engineers are highly adept at **identifying security threats** to save your in-house teams thetime-consuming and complex task of investigating real-time and historical network events to identify genuine threats from false positives.

By deploying many of these key components **in line with your existing security measures,** coupled with a highly considered hosting environment (cloud, dedicated or colocation), this can significantly increase your protection from the most common types of cybercrime helping you to protect your organisation's data, assets, brand and reputation.

FREEDOMTECH SOLUTIONS

+44 (0) 0203 917 1777
sales@freedomtech.solutions
www.freedomtech.solutions

TECHNOLOGY SECURITY

Every organisation in the UK faces the difficult challenge of mitigating against the everincreasing risks associated with cybercrime. Cyber attacks use advanced technology to exploit the vulnerabilities in your IT system to steal confidential information and disrupt your essential operational activity.

Effective cybersecurity requires a holistic, an integrated approach that involves the identification, detection and removal of cyber threats. It requires the continual update of preventive measures (controls) and regular testing to ensure that these measures are working correctly.

FREEDOMTECH SOLUTIONS

+44 (0) 0203 917 1777
sales@freedomtech.solutions
www.freedomtech.solutions

TECHNOLOGY SECURITY

NETWORK SECURITY

Network security is used to prevent unauthorized or malicious users from getting inside your network. This ensures that usability, reliability, and integrity are uncompromised. This type of security is necessary to prevent a hacker from accessing data inside the network. It also prevents them from negatively affecting your users' ability to access or use the network. Network security has become increasingly challenging as businesses increase the number of endpoints and migrate services to the public cloud.

ENDPOINT SECURITY

Endpoint security provides protection at the device level. Devices that may be secured by endpoint security include cell phones, tablets, laptops, and desktop computers. Endpoint security will prevent your devices from accessing malicious networks that may be a threat to your organization. Advance malware protection and device management software are examples of endpoint security.

CLOUD SECURITY

Applications, data, and identities are moving to the cloud, meaning users are connecting directly to the Internet and are not protected by the traditional security stack. Cloudsecurity can help secure the usage of software-as-a-service (SaaS) applications and the public cloud. A cloud access security broker (CASB), secure Internet gateway (SIG), and cloud-based unified threat management (UTM) can be used for cloud security.

INTERNET SECURITY

Internet security involves the protection of information that is sent and received in browsers, as well as network security involving web-based applications. These protections are designed to monitor incoming internet traffic for malware as well as unwanted traffic. This protection may come in the form of firewalls, antimalware, and antispyware

APPLICATION SECURITY

With application security, applications are specifically coded at the time of their creation to beas secure as possible, to help ensure they are not vulnerable to attacks. This added layer ofsecurity involves evaluating the code of an app and identifying the vulnerabilities that may exist within the software.