KASPERSKY JARGON BUSTER

YESTERDAY

UTM

UTM stands for 'Unified Threat Management.' It's a suite of security products suited for small and midsized businesses. The hardware acts as a barrier between the external environment and corporate networks, and has features that include antispam filters, firewalls, web gateway security, and other ways of keeping systems safe and secure.

FIREWALL

A firewall is a software or hardware appliance that controls and monitors access to a network. Firewalls are critical when connecting to the Internet as they can screen traffic and ward off threats to a local network. Classic firewalls are viewed as inflexible because they need to be configured manually by an administrator.

AD SPAM

Ad spam is the suspicious-looking mail that's often filtered through to your junk inbox. Real spam is characterized by being anonymous, unsolicited and sent in huge quantities - due to the fact that only a very small number of people respond to them. Marketing materials such as newsletters may resemble spam, but where a user has opted to receive them, they're legimitate mail.

APT

APT stands for 'Advanced Persistent Threat.' These attacks focus on penetrating specifically chosen systems and have a particular purpose in mind. They're usually directed by humans rather than automated and are characterised by being highly sophisticated, covert and taking place over a sustained period of time.

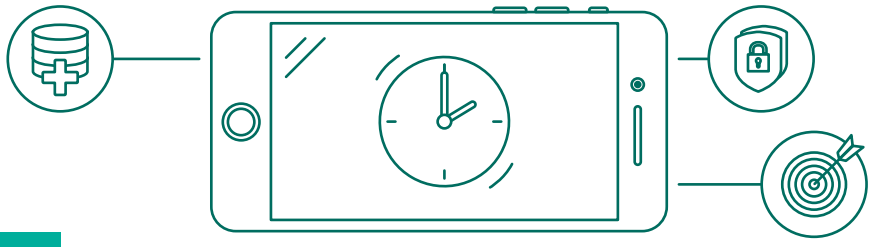
ANTIVIRUS

Antivirus software has one mission: to find and remove harmful code. At the centre of the software is the engine – a purpose-built module versatile enough to work with many products, from personal devices to mail gateways or proxy servers. The quality of the antivirus engine is determined by its ability to detect malicious code and protect the systems it's installed on.

SIGNATURE DETECTION

Signature detection is a way of protecting systems by recognising indicators characteristic of particular malware. Network indicators associated with malware can be pre-configured, so when the software detects them, they can quickly be blocked.

TODAY



MACHINE LEARNING

Applied to cybersecurity, Machine Learning algorithms enable the detection of previously unknown malware threats by 'learning' from relevant big data threat intelligence and building effective detection models. These models can be used to detect unknown malware on a company network or in a lab setting.

TARGETED ATTACK

Targeted attacks focus on a specific organisation or industry. Perpetrators plan attacks in advance, making use of phishing messages or system vulnerability to achieve their goals. Their focused nature isn't unlike APTs, with the major difference being targeted attacks aren't as costly, and may require only average skills.

BIG DATA

From a business perspective, 'Big Data' refers to the practice of using high-end technologies to analyse, query and extract meaning from the massive volumes of data a business generates. Without these technologies, companies could miss gaining valuable business insights from data that traditional applications lacked the power to process.

AI

AI refers to 'Artificial Intelligence'. An ever-advancing field, AI technology seeks to replicate the human ability to learn, come to their own conclusions, understand complex ideas, and talk naturally with other humans. As AI technology advances, it can replace humans in performing more complex, non-routine tasks.

RANSOMWARE

As the name implies, ransomware is a type of malware that seeks to extort a ransom from the victim. Ransomware starts by covertly infecting the victim's device (whether it be a computer, mobile phone, or appliance), before threatening to destroy, publish, or deny access to files unless a payment is made.

DDOS

DDoS stands for 'Distributed Denial-of-Service' attack. DDoS attacks work by flooding the targeted machine or resource with a huge amount of requests, effectively overloading the system and preventing any legitimate requests from being fulfilled. This stops the system from connecting to the Internet and renders it useless for the user.

NEXT-GEN

Next-gen is short for 'next generation' - a term used by some cybersecurity vendors to differentiate their offerings from competitor products. Often used as marketing ploy to make a product sound more revolutionary than it actually is. The best way to cut through this hype is careful study and independent testing.

MOBILE/MOBILITY

Mobility refers to the way laptops and smart devices mean employees are no longer anchored to their desks. Cloud computing has further transformed workplace flexibility, enabling people to access data from anywhere.

CYBERFRAUD

Cyberfraud refers to the use of Internet-based services and software to deceive people out of money, goods or sensitive information. As constantly evolving threat, it costs billions of dollars globally every year.

MULTILAYER PROTECTION

Sophisticated cyberattacks try to evade existing protection. Multi-layered security provides effective defense against this by securing every level of IT infrastructure with a mix of integrated security components – if one layer is breached, another is there to back it up.

EDR

EDR stands for Endpoint Detection & Response. As advanced threats such as targeted attacks become more likely, greater visibility and response capabilities are needed across the whole IT network. EDR addresses this with the emphasis on the endpoint. It uses system events to help re-create an attack picture and provide automated containment of cyberattacks.

TOMORROW

BLOCKCHAIN

Blockchain is basically a digital ledger on which transactions (such as Bitcoin, but potentially any exchange in value) can be recorded. The benefit of Blockchain technology is that while it is all publicly visible, it isn't stored in any centralised location, meaning it cannot be hacked or corrupted.

FULL-BIZ BLACKMAILING

As the world becomes more digital, businesses in the future will start to become virtualised, residing fully in public clouds. Full-biz blackmailing refers to the risk that a cyberattacker will potentially be able to take control of an entire businesses (rather than just a system or server), deny access and then demand a ransom.

PUBLIC CLOUDS

Public clouds offer all the benefits and scalability of cloud computing – delivered and managed by a service provider. Businesses simply rent or buy a 'slice' of the provider's cloud environment without having to invest in resources themselves.

UBA

UBA refers to 'User Behaviour Analytics'. As the name implies, UBA concerns itself with studying patterns in user behaviour. The system can then apply algorithms and statistical analysis to patterns that differ from what it has learned from users, thus detecting potential threats. UBA is used for snuffing out insider threats, targeted attacks, and financial fraud.

TRUE CYBERSECURITY

The True Cybersecurity approach combines multiple layers of technology and services with HuMachine™ intelligence to protect against every type of threat a business faces. It uses the best of human expertise and technology to deliver easy-to-use protection for every type of business, regardless of size or platform.

VIRTUALIZATION

Virtualization is the creation of a virtual version of a physical IT asset (such as a server, network or user's workstation to allow multiple entities use the same hardware). This can greatly increase resource efficiency and creates great flexibility in management; machines and networks can be automatically created, deleted or reconfigured according to business needs.

SECURITY INTELLIGENCE

Security Intelligence (SI) provides actionable insight into threats and helps reduce external threats to a system. This is primarily done through the real-time collection and analysis of data generated from users, applications, network flows and other infrastructure.

HUMACHINE

HuMachine™ Intelligence is a unique combination of human expertise, machine learning algorithms and big data threat intelligence to protect users from advanced and 'next-gen' threats.

MSSP/OUTSOURCE

MSSP stands for 'Managed Security Service Provider', and refers to the outsourcing of the management, monitoring and incident response to a third party provider. This ultimately relieves businesses of the need to hire and train in-house security staff.

DIGITAL TWIN

A 'Digital Twin' is a computerized version of a physical object. It uses sensors to collect real-time information about the physical object that can be used for status, monitoring or control via a computer – this is particularly useful for, say machine parts or high-tech medical devices that are hard to visually assess.

INTERNET OF THINGS (IOT)

The Internet of Things (IoT) is where devices such as thermostats or fridges are embedded with technology that allows them to connect with the Internet, enabling remote control and communication between them.