Network security is key throughout government and military forces the world over

Militarisation of cyberspace requires more vigilance for IT networks

Network security is key throughout government and military forces the world over, and it's becoming an increasingly complex feat to achieve. Information is fast being considered every bit as deadly as actual artillery. Here, Paul Darby, Regional Manager, EMEA at Vidder, outlines the ins and outs of keeping critical networks secure, and reports on Operation Convergent Response, where new and effective cybersecurity solutions were proven.

Information is, more often than not, the single most important factor when it comes to military victories. Strategic intelligence, battle plans, troop manoeuvres and the location of supplies are converted digitally so that they can be distributed to command posts using cable, satellite and radio. The importance of this information cannot be over emphasised, its impact considered so crucial that it is classified in the same category as artillery - as a deadly long-range weapon.[1]

How this information is stored and accessed is constantly evolving as the military slowly migrates to the types of systems commonly used by commercial operations. It was only last year, for example, that the British Ministry of Defence (MoD) moved its computing away from the secure internal legacy network it had used for the previous decade to take advantage of the first Microsoft data centres to open in the UK.

With such a move comes concerns about security. Despite the many security protocols that accompany the storage and access of highly sensitive data such as banking details or personal health records, the impact of a breach of military information could undermine command and control infrastructure and cost countless lives.

Cyber espionage

Warfare today takes many forms, and one of the most insidious is not on the physical battlefield at all, but from malicious hackers sitting behind a computer screen with an eye on any chink in crucial IT networks. In its annual Data Breach Investigations Report, communications giant Verizon said that whilst around 73 percent of breaches are financially motivated, 21 percent are related to cyber-espionage. An increasing number of these are politically motivated or state sponsored, and this has implications for military forces across the globe.

Ukraine is a good example of how cyber attacks on IT networks have had a long-term and serious impact. Over the past three years, the country has suffered repeated hacks on military, finance, transport and political targets, eliminating data and destroying computers. In June of this year, the severity of a hack that caused government ministries to shut down in Ukraine, prompted NATO's Secretary General to warn that a cyber attack could trigger Article 5 of the north Atlantic treaty in the same way as a conventional military assault.

According to the Daily Telegraph, the same attack saw the British Defence Secretary, Michael Fallon, state that the UK would consider retaliating militarily against a cyber attack by another state.

The growing militarisation of cyber space has put more pressure than ever on the security of IT networks ironically at a time when digital transformation is opening up access to military personnel. It was over four years ago that the Pentagon approved iOS 6 mobile devices for use when connecting to defence department networks. Military-specific virtual private networks have also become more and more common in recent years, improving communications and remote access to crucial data with an additional layer of protection.

Adopting zero trust

Of course, successful civilisations work in an atmosphere of mutual trust, and, given that we are living in a digital age, any lack of trust has the power to undermine progress. However, the biggest challenge we face in the current cyber war is that we can't identify the enemy, which means trust has to be given with great caution, if at all.

Military communications are improved and enhanced through access to digital applications, devices and cloud computing, but a balance needs to be struck to ensure that this valuable access is totally secure and strictly controlled.

The only way to do this is through systems that provide granular access controls to assets based on trust. Access should be permitted only on the basis of having a deep knowledge of where a connection initiates from and where it is going to, validation of relevant credentials and continuous monitoring to ensure it is restricted only to approved assets.

Sharing data and opening up communications also means exposing IT systems to the growing community of cyber attackers and their sponsors. When this data includes important military strategy, we simply cannot afford to do this lightly. A zero trust approach is the only way that, for now, we can protect ourselves against the stealthy but determined creep of cyber warfare.

A case in point – Operation Convergent Response

Currently information solutions for first responders, the medically trained team that are first on the scene of an accident, incident or event, are built using customised, highly complex and costly communications and application systems. While the adoption of mobile devices and public clouds have become the norm for enterprises, these have, until now, been considered too risky for emergency services.

Global communications company Verizon recently carried out 'Operation Convergent Response' (OCR), and it was the first large-scale demonstration of how IT networked services could be used to instantly provide information to the vital first responders team. OCR brought together experts in emergency response and communications for two days of hands-on exercises. A key aspect of OCR was to showcase how Verizon's LTE service combined with a concept called Software Defined Perimeter (which works on the principle of allowing access to the network on a 'need-to-know' basis) enabled secure connectivity between emergency response personnel, surveillance equipment and cloud-hosted applications.

Event communication was provided by Verizon's truck-mounted LTE tower, which is designed to provide instant voice and high-speed data coverage during emergencies. Surveillance drones and robots transmitted live video to a Microsoft Azure cloud-based command centre using Verizon LTE. First responders were able to access hosted applications utilizing Verizon's new SDP service.

Operation Convergent Response featured many real-world scenarios including a subway accident, flood and chemical spill. The most exciting event, however, was a hostage rescue demonstration using a drone to air drop a robot with high resolution imaging onto the roof of a building. The video stream was sent to hosted apps that were protected by Verizon's SDP service. The enhanced situational awareness provided security personnel with high resolution targeting information.

One of the technical highlights of OCR was how Verizon is applying the Software Defined Perimeter (SDP) principle built on Vidder's PrecisionAccess managed security service. This verifies the user and device identity before granting mission-based access. A certificate-based mutual TLS virtual private network ensures that connections cannot be intercepted when first responders connect to hosted application resources. To stop malware from spreading through network connections, the SDP provisions all connectivity at an application layer i.e. from the 'app inside' the user's device to a specific port of a server. Any malware on the user's device is outside the application layer tunnel. Also demonstrated was the new remote trust assessment inspection capabilities of the SDP service.

The combination of SDP's strong security model combined with Verizon's LTE coverage allowed the first responders to securely access critical information on their mobile computing device. The blending of multiple services created a fully integrated on-demand command and control system that was well received by event participants. OCR successfully proved that public communications and computing services offer first responders a more effective approach to information collection,

Left to right Jeff Schweitzer of Verizon, Vidder's CTO, Junaid Islam and Jad Muntasser of Verizon

processing and distribution than legacy hardware-based solutions.

Behind Operation Convergent Response was valuable military experience. The exercise was developed and led by Jeff Schweitzer - Verizon Enterprise's Chief Innovation Architect. Prior to joining Verizon, Jeff served in the US Army and Pentagon as a communication expert. To ensure that OCR scenarios reflected real world challenges Jad Muntasser, a former Navy Seal and a leading expert in anti-terror and hostage rescue operations, helped create the scenarios. Both Jeff and Jad have extensive combat experience and have continued their commitment to public service in private life. **GMC**

[1] *Joint Pub 3-09, Joint fire support, "conduct information operations" is a key fires task on a par with "conduct fire support" using artillery and airstrikes*

Shawn Hakl, Vice President, Verizon

Survivor R ready to roll – Rheinmetall delivers two special ops vehicles to the Saxony State Police

On 15 December 2017 Rheinmetall transferred the first of two heavily protected Survivor R transport vehicles to the Saxony State Police. The second system was delivered before Christmas. The Free State of Saxony ordered the two vehicles from Rheinmetall MAN Military Vehicles (RMMV) in February of 2017. Forming part of an extensive anti-terror package, the vehicles will be used to equip special police units in Saxony.

The Survivor R is a compelling symbol of Rheinmetall's extraordinary expertise in the worlds of security and mobility. Developed in cooperation with Achleitner, a maker of special vehicles, it is the perfect answer for robust law enforcement operations. Vehicles of this type are especially important in high-risk situations when police special operators have to be safely transported to the area of operations or for evacuating persons from the danger zone.

Among other things, Saxony's two Survivor R vehicles feature a special signalling system; an integrated, remotely controlled observation turret with optronics and effectors; a high-performance loudspeaker; and a hydraulically operated rear ramp for rapid entry and exit. A powerful 340 HP engine with torque of 1,250 Nm gives the 17-tonne vehicle an outstanding mobility. Moreover, the environmentally friendly Survivor R meets the latest Euro 6 emission norms.

The armoured monocoque cabin provides the crew with all-round protection from multiple threats. Ergonomically designed, the well-lit interior offers sufficient space for crewmembers and their personal equipment as well as extensive communications and command and control technology.

Systematic use of serially produced, standard commercial and military components has resulted in a reasonably priced vehicle – one which benefits from Rheinmetall MAN's global service network, assuring efficient maintenance and repairs worldwide. This makes the Survivor R a cost-effective, easy-to-maintain vehicle platform with low lifecycle costs and outstanding operational readiness. The Berlin State Police have also ordered the Survivor R. **GMC**

SpacePath COMMUNICATIONS

Best in class - size, weight and power performance

Outdoor High Power Amplifiers

- 1250W, 750W, 400W, 180W
- C, X, Ku, DBS & Ka-band

Indoor Touch Screen Amplifiers

- 1250W, 750W, 400W
- C, X, Ku, DBS & Ka-band
- 1:1 & 1:2 Systems

Outdoor HPA Systems

- 1:1, 1:2 Redundant & power combined systems
- Small, lightweight
- Easy maintenance

Outdoor SSPBs

- Ka-band 10, 20, 40W
- Ku-band 16-200W
- C-band 40-400W

Come see us at:

CABSAT
Stand Number: ZB1-C33

26th Convergence India 2018
Stand Number: E277

SATELLITE 2018
Stand Number: 114

Spacepath Communications www.space-path.com / +44 1256 760525