kapsch

Five Top Tips for Maximising Network Security

InterComms talks to Mario Tscherwenka, Technical Solution Manager and Security Specialist, Kapsch CarrierCom, about enhancing network security and performance in the IP era

Kapsch CarrierCom is an independent systems integrator for public fixed and mobile operators, providing unbiased, end-to-end support for multi-vendor network deployments.

Large-scale migration to complex, converged IP networks have increased network security risks by orders of magnitude. To close complex security loopholes and maximise network efficiency, operators need sophisticated, multi-layered security solutions that are designed to meet their specific needs, says Mario Tscherwenka, Technical Solution Manager and Security Specialist at Kapsch CarrierCom.

The evolution of carrier networks towards all-IP transmission is driving fundamental changes in the security and risk landscape. In particular, IP network elements, such as the IMS for Voice over IP services, have become a focus for malicious attacks. In addition, the variety of transmission protocols, including Carrier Ethernet, MPLS, Multicast and others, are increasing network complexity and opening new loopholes for cyber criminals to exploit.

Widespread virtualisation of carrier networks (SDN, NFV) also presents a number of new security threats for operators. To ensure that revenue-generating, customer-facing services remain available, virtualised infrastructure components that are controlled by the constant interchange of messages must be protected from both internal and external interference.

In addition to increased network complexity, the proliferation of network access devices also poses new security challenges, with more than 2,000 new Android devices registered on UK mobile access networks in the last two years. Many of these devices, and the applications running on them, behave in ways that, left unchecked, could overload border and core systems and influence OSS/BSS services that rely on them.

Malicious activity on mobile access devices is, of course, another key concern for operators. Users may try, for example, to gain unauthorised access to network services using a mobile device, or to use other mobile devices on the network to deliver spam messages. In addition, hackers regularly perpetrate zero-day attacks to exploit software issues, while their worms and viruses initiate high volumes of messages with the intention of overloading core network infrastructure components. The ability to control and prevent this kind of malicious activity is now vital for effective revenue protection.

Five steps to a secure IP infrastructure:

1) Build a bespoke security infrastructure that is fit for purpose

Many network security providers take a 'one-size-fits-all' approach, using security devices to screen traffic at the core network and aggregation layers. However, the size and complexity of today's all-IP networks, and the myriad of network elements and access devices, means that this strategy is no longer effective.

To close all the security loopholes, it is necessary to first conduct a thorough audit of network components and interdependencies. By doing this, carriers can design and implement a bespoke security solution that is mapped to the carrier's specific environment. This approach ensures that security devices are placed correctly in the network and configured properly, maximising protection against malicious attacks.

2) Choose flexible solutions that can adapt to evolving security threats

Operators are constantly reacting to new security threats caused by either malicious attacks, such as zero-day attacks or denial of service attacks, or by negative subscriber, application or device behaviour. With no visibility of where the next threat is coming from, network security solutions need to be extremely agile.

This need is not currently being met by traditional network security companies, who tend to focus on either data centre and enterprise security, or mobile network security – but not both at the same time. With evolving security threats potentially impacting multiple areas of the carrier network, vendors of 'single domain' security solutions may not be able to support operators in a timely manner, and there may be unwanted delays or issues before security holes are plugged.

To maximise flexibility and network protection, carriers should look at vendors and solutions with the broadest possible scope of security capabilities. Ideally, solutions should be based on proven enterprise and data centre technologies, but extended with the full range of carrier security features and reliability. All key areas of the network should also be covered, from the core network, access network and aggregation layer, to mobile management components, and more.

3) Block unwanted traffic to maximise operational efficiency and revenues

A range of traffic types threaten network security and efficiency, from SIG messages and other service requests generated by hackers, to diameter traffic generated by foreign-controlled networks to support mobile roaming capabilities. The key to increasing operational efficiency and network performance is to analyse and mitigate this traffic before it impacts core network elements.

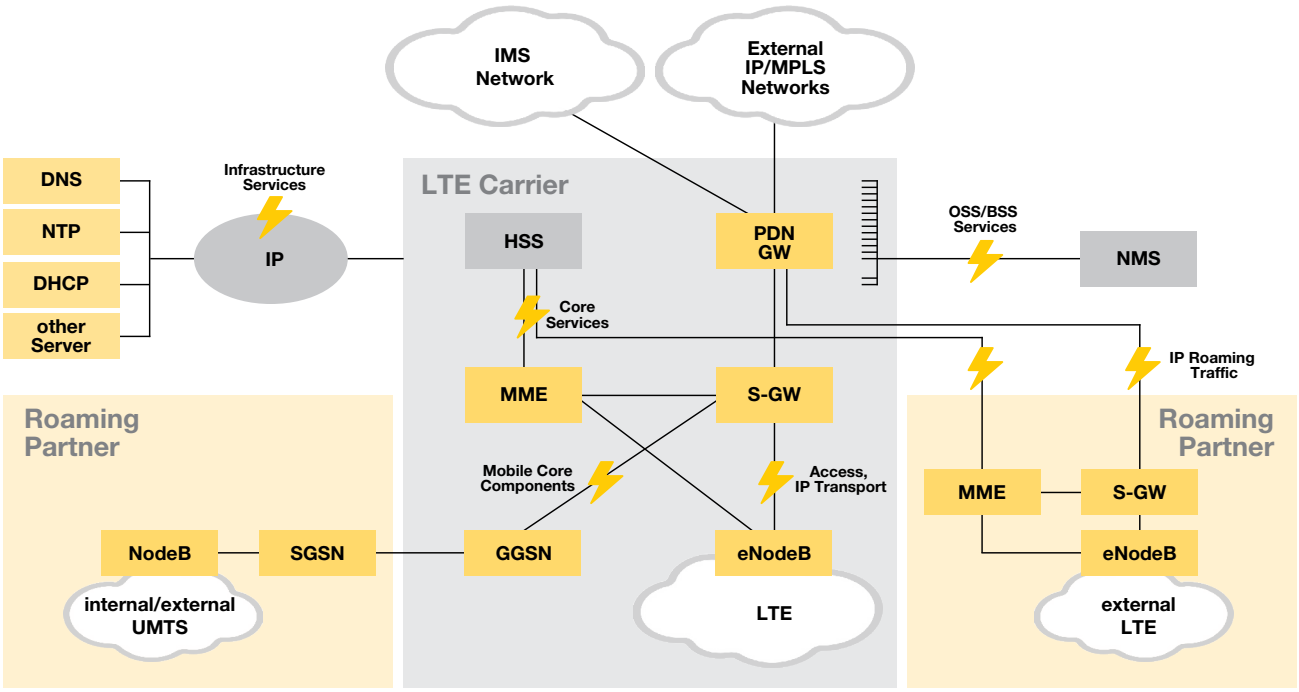
As well as using security solutions at the aggregation and core-network layers to block malicious traffic, carriers may also choose to reduce traffic using message filtering. Messages can be filtered, for example, to block irrelevant messages and ensure that only relevant messages are delivered, significantly reducing network traffic and costs and freeing resources for revenue-generating services.

4) Generate revenues with customer-facing security services

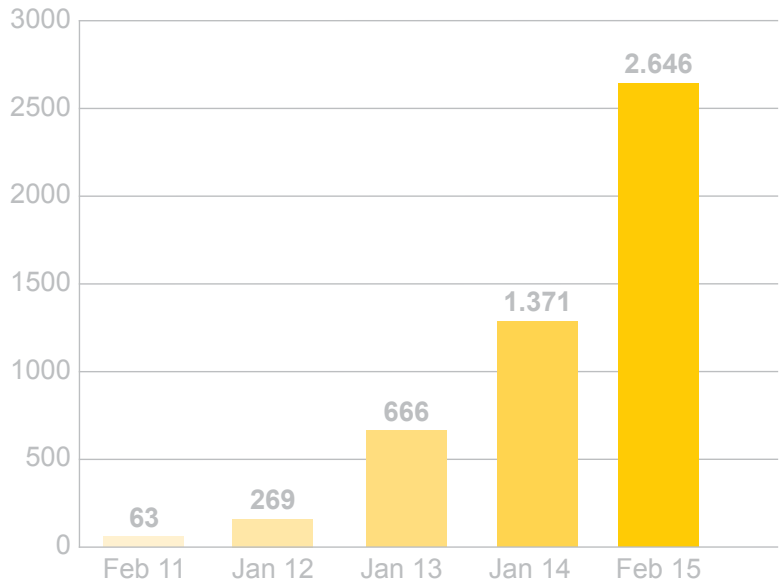
The implementation of next-generation security solutions for IP networks logically implies significant initial technology investments. However, carriers can leverage this infrastructure to deliver value-added security services to their customers, generating significant revenue streams in the process.

The ability to detect viruses and malware at a central level, for example, means that operators could sell anti-virus services for customers who don't want to install heavy, battery intensive anti-virus programs on their

Security Threats in the LTE Network



LTE User Devices Growth
Source: The Status of the LTE Ecosystem by GSA



smartphones. In addition, carriers could sell protection against other types of risks, such as phone hacking to send spam messages.

5) Adopt a 'phased' approach for network security deployments

By taking a phased approach to deploying network security solutions, carriers can generate the greatest possible returns on their investments, while minimising negative impacts on day-to-day processes.

A phased deployment might initially focus on addressing a specific and pressing security challenge, such as hackers using mobile devices to scan for open IP ports with the intention of accessing particular applications and services. In this example, a denial of service mitigation system could be deployed first to address the problem and free up radio resources for revenue-generating customers.

For future, less pressing phases of the deployment, carriers may choose to implement additional security functionality such address matching to enhance network protection, for example based on more effective malware detection.

Maximising network security and performance with Kapsch CarrierCom

For decades, Kapsch CarrierCom has been helping operators to optimise security across all layers and components of their networks. We take the time to understand each carrier's network, build simulations of IP network element or virtualised infrastructure as required, and design bespoke solutions that maximise protection against malicious attacks and negative subscriber and device behaviour.

Because Kapsch CarrierCom is vendor independent, we can deliver best-in-class security solutions that safeguard all areas of the network, from core systems and aggregation systems, to mobile access networks. By seamlessly integrating the best data centre security and carrier security solutions, we can ensure that networks are protected against all kinds of malicious attacks, whether internal or external, both now and in the future.

Over the years, we have implemented network security solutions for major carriers across Europe and worldwide. We specialise in taking a phased, incremental approach to delivering network security, helping our clients to achieve maximum impact from their security spend and minimising impact on day-to-day activities.

For more information visit: www.kapsch.net/kcc

or contact us at: kcc.carriers@kapsch.net