Security Gets Dedicated Work Package in GN4-3 Project

The security and integrity of the GÉANT and NREN networks and their services have always been essential elements of the GÉANT project, but until now this work had been distributed across a range of Service Activities and supported on a voluntary basis through various Task Forces and Special Interest Groups. Now, reflecting the increasing emphasis on proactive security across the NREN community, all these disparate activities are being consolidated under a new work package (WP8) as part of the GN4-3 project.

WP8 brings together 43 people from 19 different organisations making it one of the most distributed and inclusive work packages within GN4-3. This breadth of contributions is one of the work package's core strengths; By combining expertise and skills from across the community, WP8 aims to become a centre of excellence for networking security and will enable knowledge transfer between NRENs.

Such knowledge transfer is crucial because, regardless of their size, all NRENs are facing very similar threats and for each organisation to have to climb the same learning curve independently can be costly and mean that many could be left vulnerable for longer than necessary.

The main work streams within WP8 are covered by three tasks, each focused on a different aspect of security: Business Continuity, Security Baseline and Products and Services.

Business Continuity (T1)

The business continuity task focuses on supporting NRENs and Institutions in a range of areas including:

- Security Awareness – consolidating this aspect across the community considerably lightens the individual workload in terms of security management for each NREN.
- Training, particularly Crisis Management – the worst possible time to learn how to manage a security incident is in the moment when it happens, so it is very important that different team members across various areas (NOC, IT, PR and Management) be trained to understand their roles and responsibilities should a major incident occur.

- Evaluation and Sharing of Best Practices – The NREN community is very diverse (particularly in terms of languages) and organisations may have different experiences and skill sets when it comes to security. Nevertheless, the threats they face are similar, so formalising knowledge on methodology to mitigate risks into best practices will enable individual NRENs to benefit and avoid steep learning curves when faced with each new technology or threat.

Security Baseline (T2)

In order for NRENs and institutions to understand how to enhance their security policies, it is essential to first assess where they stand currently and where to focus efforts. The security baseline task will help build sample security checklists to identify the key areas where NRENs can make the biggest improvements.

Security work can often seem like a never-ending arms race, with attackers finding and developing new ways to attack networks and services all the time, making the task of keeping track of the threat landscape daunting and time-consuming. The team will work to identify the 10 greatest areas of risk for NRENs and work with Task Forces and Special Interest Groups (especially SIG-ISM) to keep up to date with the latest security threats and relative counter-measures.

Leveraging skills and expertise across the community and helping communicate outcomes and results via the SIGs and TFs will ensure that all NRENs, and not just those in a position to contribute resources, will benefit from this work.

Products and Services (T3)

The products and services task will be supporting the development of a range of new security and security-related services to support NRENs, institutions and end-users, including:

- SOC Tools – A range of tools to help NRENs build efficient Security Operation Centres will be made available across the community.
- Vulnerability Assessment as a Service – A common framework for vulnerability assessment tools will help NRENs ensure that their networks and services are protected against many external threats.
- DDoS Mitigation – Distributed Denial of Service (DDoS) is a major and growing concern for all network-based organisations and services, as these types of attacks can be easy to implement and can damage not only the system or location under attack but also have major knock-on effects across the whole network. Tools to help mitigate these attacks will therefore be developed to support SOCs.
- Firewall on Demand (FoD) – Firewalls can protect individual services from a wide range of attacks but as attacking traffic traverses R&E networks it can interrupt other services. FoD seeks to block attacks, especially DDoS-related ones, closer to their source so as to reduce their impact on R&E networks.
- eduVPN – End users also require security and privacy and using third-party networks can expose them to several risks. Opening up institutional services to access from third-party networks can also expose them to attack. eduVPN allows users to connect securely to the Internet and services to better control access to protect themselves from external threats.

Network and service security is an ever-evolving field and can consume vast amounts of resource within NRENs and Institutions. By instituting the Security Work Package in GN4-3, GÉANT hopes to work with the community to provide a hub of expertise and give NRENs access to the latest security knowledge, skills and tools by the most effective means possible.

For more information about the work of the GN4-3 Security work package see **https://wiki.geant.org/display/gn43wp8/GN4-3+Security+Workpackage+WP8**

eduVPN – Providing Extra Security and Privacy for Mobile Researchers and Students

With tens of thousands of hotspots in over 100 countries, eduroam has become an invaluable tool for every mobile student and researcher. However, when eduroam is not available or an additional layer of security and privacy is needed, the question how to protect your privacy when using public WiFi becomes an issue.

Although VPN services can help, they are not without pitfalls. Commercial VPNs may still leave you exposed or generate a digital footprint of your access. Also, if you need to access services inside your institutions network, public VPN access may not be sufficient. This is where eduVPN provides a solution that addresses these issues.

As part of the new Security Work Package in the GÉANT project, eduVPN has been adopted by a number of R&E institutions as their enterprise VPN solution and an increasing number are considering eduVPN as the solution for giving their users secure access to protected resources on their internal networks.

Using a fully open source solution that has been developed by the NREN community and been subject to a robust auditing process (both the server and clients have been audited multiple times) is usually attractive to institutions. In addition to providing strong encryptions, eduVPN offers a number of compelling features. It provides full IPv6 support, both inside and outside the tunnel (providing IPv6 addresses to clients and connecting to the server over IPv6). It also integrates with existing identity managements systems using SAML, LDAP or Radius. Another major benefit eduVPN offers NRENs and institutions is the support for generic hardware to operate the VPN gateway. New features do not require a new VPN box, instead the open-source software can simply be upgraded. Where additional VPN capacity is needed, it is easy to add additional CPU cores or bandwidth.

For end-users, there are other benefits, in particular the user-friendliness of the apps. Inspired by the idea that VPN configuration should be simple on any device, once authenticated through their federated identity, eduVPN users can configure their device, activate or deactivate a VPN in just a few clicks. eduVPN apps for Windows, macOS and Android have been available for some time and, following the successful resolution of some licensing issues, an iOS app became available in March 2019. Native applications are available for all major platforms.

In addition to connecting to protected resources at institutions eduVPN also increases security when surfing the web. On selecting a national instance in the apps, which is typically operated by an NREN, the user can route their traffic to the Internet via a VPN to a trusted gateway. The number of national instances used to connect to the Internet is growing, and this is particularly useful when connecting on an unsecure network – for example a public WiFi network where eduroam is not available. As an added benefit the client can use IPv6 and if the network is restricted in some sense, circumvent that.

Last but not least, on these national instances, all current operators have chosen to allow “guest usage”. This permits the user to route their traffic via eduVPN to a gateway to the Internet operated by their own NREN or by a participating NREN in another country. Using this eduroam-inspired approach, eduVPN enables easy, secure and free access to Research and Education networks.

For more information visit: **eduVPN.org**