Lecciones aprendidas en materia de seguridad en las universidades españolas durante la crisis del covid-19

Caso de uso en la Universidad de Sevilla

La situación derivada del **COVID-19**, ha permitido, al mismo tiempo, a las universidades, organismos y compañías extraer valiosas lecciones que permiten afrontar el futuro inmediato bajo la convicción de que era necesario un replanteamiento: las actividades docentes deben llevarse a cabo de manera segura y la actividad en los centros universitarios debe adaptarse en consecuencia a estas medidas *("Recomendaciones del Ministerio de Universidades a la Comunidad Universitaria para adaptar el curso Universitario 2020-2021 a una presencialidad adaptaba").* El caso de la **Universidad de Sevilla** es un buen ejemplo de adaptación a la nueva realidad en materia de seguridad de redes.

El caso de uso de la Universidad de Sevilla: visibilidad de la superficie de exposición (todos los dispositivos conectados a la red) en un momento crítico y adaptabilidad para la vigilancia de los accesos remotos.

Los números de la Universidad de Sevilla:

+100K	70.000	4.200	2.600	32	7
Dispositivos conectados	Alumnos	Docentes e investigadores	PAS	Centros Universitarios	Campus

La Universidad de Sevilla es la tercera Universidad con más alumnos de España

La Universidad de Sevilla es la tercera Universidad más grande de España por número de alumnos y la segunda en modalidad presencial, sólo superada por la UNED y la Universidad de Barcelona. (Fuente: Statista, Ranking de las Universidades Públicas de España con mayor número de Alumnos, 2020). Esta Universidad cuenta con cerca de 80.000 usuarios (70.000 alumnos y 8.000 empleados) distribuidos en 7 campus.

La necesidad por parte de la Universidad de Sevilla es clara: **dar una buena calidad de conexión a todos los usuarios al tiempo que se asegura la red.** El problema identificado por parte de los administradores de redes es el alto nivel de redes públicas cableadas que existen en la infraestructura de la Universidad, ya que el personal del centro docente valora la facilidad para conectarse a la internet sin medidas especiales de seguridad (con el riesgo que esto supone para la preservación de la confidencialidad de los datos de alumnos / investigación y la superficie de exposición a brechas de seguridad que comprometan la reputación).

"Nos dimos cuenta de que nuestro mayor problema era que no sabíamos qué estaba conectado a la red de la Universidad. Adicionalmente, queríamos tener control sobre ello. Por ejemplo, no podemos pedir a alumnos ni personal que utilicen un determinado antivirus, pero con EMMA podemos impedir el acceso a la red a aquel que no cuente con uno".

(Pablo Tenorio, Jefe de Sección de Redes en la Universidad de Sevilla)

En este contexto y con una red tan extensa (50.000 puntos cableados y 1.200 puntos de acceso), la Universidad de Sevilla carecía de visibilidad sobre aquello que estaba conectado. Aunque se habían tomado medidas de seguridad perimetral, eran conscientes de que en muchas ocasiones la mayor exposición al riesgo se encuentra en los dispositivos dentro de la red de la Universidad.

La solución EMMA-VAR del CCN-CERT dio a la Universidad de Sevilla visibilidad de todo lo conectado a la red, descubriendo más de 100.000 dispositivos en poco tiempo (+70.000 dispositivos descubiertos en la primera semana) y realizando un perfilado de los mismos, permitiendo alcanzar el objetivo del centro universitario: filtrar los accesos internos para garantizar la salud de los mismos antes de acceder a la red.

"Nuestros mayores esfuerzos se concentran en el reto de securizar el tráfico y adaptarnos al ENS. Nuestra Responsable de Seguridad hace hincapié constante en la necesidad de adaptarnos al mismo".

(Pablo Tenorio, Jefe de Sección de Redes en la Universidad de Sevilla)

Descubrimiento y perfilado de dispositivos en la Universidad de Sevilla en una semana

La llegada del covid-19 y la adaptabilidad de EMMA: vigilancia en los accesos remotos

Las necesidades de la inmensa mayoría de organismos cambiaron de la noche a la mañana y la US no era ajena a ello. El módulo de visibilidad de **EMMA** se implementó en la Universidad de Sevilla al tiempo que se iniciaban las primeras medidas de freno del **COVID-19** a nivel estatal. En esta situación, la Universidad de Sevilla contaba con una solución de VPN que utilizaban unos 500 usuarios. **De un día para otro, se vio en la obligación de prestar servicio a al menos 7.000 usuarios**. Así, las necesidades y características de la solución de VPN cambiaron.

Necesitábamos una solución robusta que permitiera el acceso remoto de 7.000 usuarios, un incremento del 1300% de usuarios conectados".

(Pablo Tenorio, Jefe de Sección de Redes en la Universidad de Sevilla)

La adaptabilidad de la solución **EMMA**, compuesta de 7 módulos, permite a los organismos adaptarse a la realidad de su contexto de seguridad. Así, ante el cambio de necesidades y prioridades provocado por el **COVID-19**, la Universidad de Sevilla optó por implementar el módulo **EMMA-VAR**: una solución robusta que permite el acceso de remoto de un número mucho mayor de usuarios a la red y que ha reportado los siguientes beneficios a la US:

- **Autenticación robusta:** perfilado y autenticación mediante el LDAP de la Universidad y el doble factor de autenticación de **EMMA-VAR.**
- **Perfilado continuo y en tiempo real:** la Universidad de Sevilla verificó los tags definiendo los parámetros mínimos de cumplimiento por parte del usuario.
- **Vigilancia del sistema:** monitorización del tráfico y del comportamiento entre el usuario de la Universidad y el sistema.

Lecturas aprendidas y conclusiones extraídas:

- **EMMA ha permitido a la Universidad conocer la superficie de exposición y adquirir conocimiento de lo conectado**, controlar la red y adaptarse a la nueva realidad dotando también de acceso remoto seguro a los usuarios.
- El **soporte y atención por parte de partner y fabricante**, quienes han mantenido un alto nivel de implicación y de especialización técnica, han sido fundamentales para la implementación de la solución.
- **Los diferentes módulos de EMMA** permitirán a las Universidades adquirir aquellas funcionalidades de la solución que mejor se adecúen a los requisitos de seguridad de la nueva realidad tras las lecciones aprendidas post COVID-19.
- **La solución permite adaptarse al ENS**, ayudando a cumplir con los principios básicos y requisitos que garantizan la seguridad de la información de los organismos.
- EMMA-VAR (Vigilancia en Accesos Remotos) y Visibilidad son dos módulos claves y **piezas estratégicas en el plan de contingencia de las Universidades** en el nuevo curso 2020-2021.

EMMA: Una solución modular que garantiza resultados en menos tiempo, minimizando la inversión económica y facilitando la operación.

EMMA es una solución encargada de la vigilancia de deficiencias en la capa de acceso y electrónica (cumplimiento), conectividad a la red (visibilidad), capacidad de respuesta ante eventos (respuesta) y acceso remoto seguro.

Al tratarse de una solución compuesta por 7 módulos (Visibilidad, Control / Respuesta, Segmentación Cumplimiento, BYOD, Gestión de Invitados y Vigilancia en Accesos Remotos), permite la inversión sólo en lo más urgente dentro del plan de contingencia con la posibilidad de establecer un crecimiento paulatino, **mostrando así resultados en menos tiempo, minimizando la inversión económica y facilitando la operación.**

Adaptabilidad y complementariedad, los principales beneficios de EMMA

Un producto que se adapta a la red de la universidad.

- Agnóstico a la electrónica de red
- Complementariedad: Se integra con otros productos ya adquiridos y con VPNs actuales y aporta información a otras soluciones

Mediante empresas certificadas por el CCN-CERT para garantizar los resultados del Plan de contingencia en tiempos y presupuestos

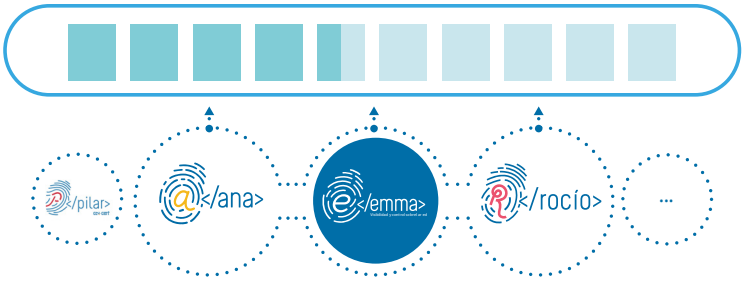
Lo estratégico Y lo táctico

Asegurar resultados (tangibles) a corto plazo **Y** crear las bases para el futuro.

ESTRATÉGICO
Esquema Nacional de Seguridad

ENS

TÁCTICO/ OPERACIONAL
Soluciones del CCN-Cert



Siguientes pasos:
Contacta **emma@ccn-cert.cni.es** para arrancar el proceso de aproximación para Universidades