EMMA: Vigilancia en accesos remotos

El Problema:

Las organizaciones están siendo impactadas de forma inesperada por la situación macro actual “COVID-19” y deben a cambiar su esquema operativo de manera urgente. Las empresas tienen que realizar estos cambios en el menor tiempo posible para asegurar la continuidad del negocio.

“Ante pandemias como la actual de COVID-19, en numerosas entidades y organizaciones se está generalizando el uso del teletrabajo como medida para evitar contagios y facilitar la confinación de los empleados.

.. numerosas organizaciones [..] han tenido que implantar en un tiempo muy reducido soluciones de teletrabajo que abarcan un gran número de aspectos: dispositivos corporativos, conexión a Internet, aplicaciones de chat y/o mensajería, videoconferencia, acceso remoto a la red y sistemas de la organización, etc.
Todo ello, sin contar con las medidas de seguridad habituales dentro del dominio de la organización y que en un tiempo récord se tienen que trasladar para seguir protegiendo la información.”

.. los ciberdelincuentes han aprovechado esta situación de vulnerabilidad para incrementar sus ataques de
todo tipo..

CCN-Cert marzo 2020

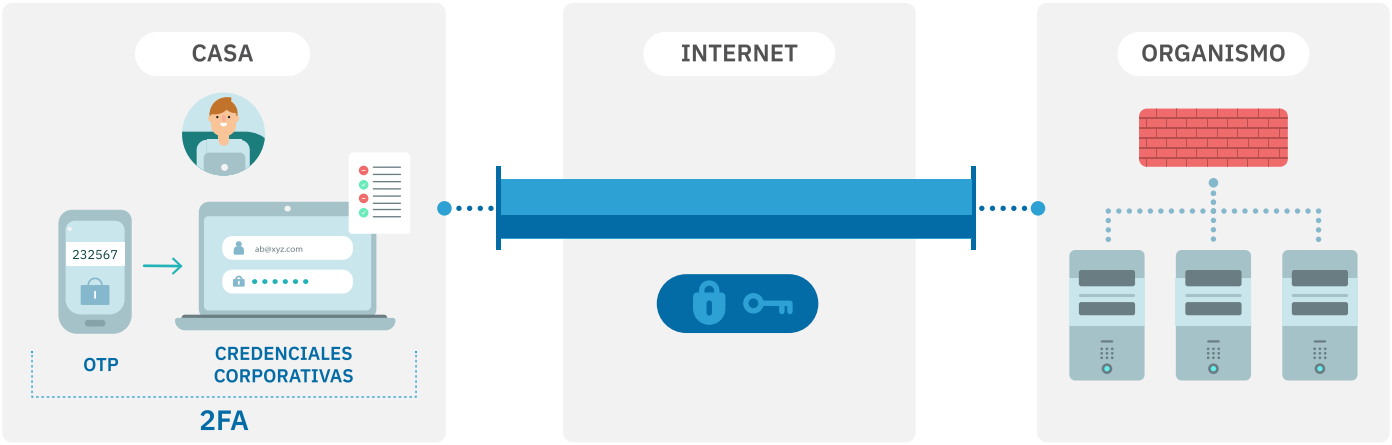
+70% *

Ataques dirigidos en el contexto Covid-19

COVIDLOCK **

Ransomware dirigido

*El Centro Criptológico Nacional ha detectado este mes un incremento de un 70% en el llamado phishing
**CNIP...COVIDLOCK es un software malicioso que es considerado especialmente peligroso para las infraestructuras críticas



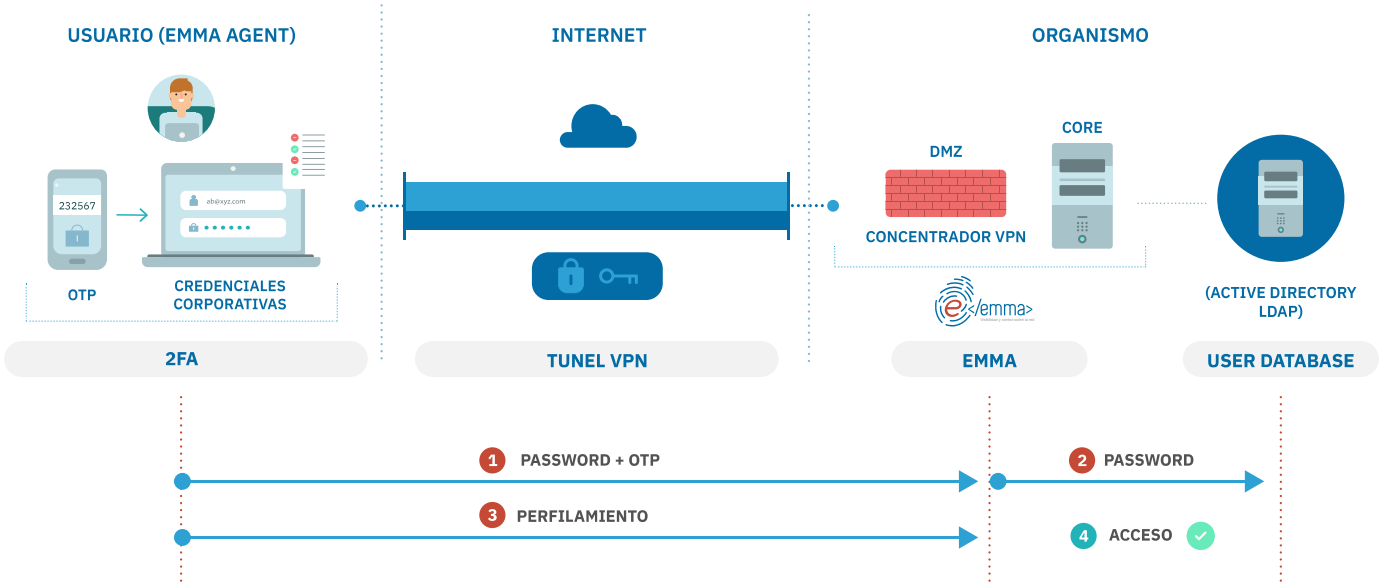
Solución EMMA: **Cumplimiento, visibilidad, respuesta y acceso remoto**

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.

Para el acceso remoto seguro, el módulo de concentración de VPNs de EMMA actúa como frontend para la finalización de túneles VPN con los clientes, mediante un agente (para dispositivos corporativos y no corporativos). EMMA realiza la autenticación, autorización y auditoría contra el gestor de identidades corporativas del Organismo (Active Directory (AD), LDAP...) y permite añadir un segundo factor de autenticación (OTP), de esta forma mitiga el riesgo de suplantación de identidad (uso de credenciales robados por parte de un atacante para acceder a la red).

Se recoge el inventario y perfilado completo del equipo. Este perfilado se podrá utilizar en las políticas de acceso a la conexión remota. Adicionalmente, permite definir y aplicar políticas de acceso en función de una postura de seguridad basada en el nivel de bastionado deseado, además de otros factores (horario de la conexión, características del equipo, role de usuario etc.). Una conexión segura y verificada de manera robusta, entre el usuario y los sistemas corporativos, monitorizando de manera continua el comportamiento de la conexión.

Arquitectura



1. El usuario envía credenciales corporativas y token (OTP) hacia EMMA para validación de identidad.
2. EMMA valida token y consulta credenciales corporativas al User Database.
3. El dispositivo de usuario envía su postura para evaluar cumplimiento de requerimientos mínimos de conexión.
4. El usuario obtiene los accesos corporativos asociados a su identidad.
5. Todo el tráfico intercambiado en la conexión VPN será monitorizado por EMMA para asistir en la identificación de anomalías en el comportamiento.

El usuario deberá instalar el agente VPN en el dispositivo que va a utilizar para realizar la conexión. A través de este llevará a cabo el proceso de validación de identidad por medio de uno o dos factores de autenticación. En caso de usar un solo factor de autenticación, utilizará sus credenciales de usuario corporativo (nombre de usuario y clave de AD / LDAP etc.) para iniciar la conexión (algo que sabe). En caso de usar dos factores de autenticación, deberá contar con Google Authenticator en un dispositivo asociado a la persona, y una semilla de token válida que permita garantizar su identidad, (OTP) (algo que tiene).

El túnel VPN se establecerá entre el dispositivo de usuario y el módulo de concentración de VPNs de EMMA. Una vez validada la identidad del usuario, el dispositivo de usuario deberá aprobar la evaluación de la postura, es decir, garantizar el cumplimiento de los requerimientos mínimos de conexión. Posteriormente se asignará un segmento de red correspondiente, el segmento asignado heredará los permisos de acceso del usuario asociados a su identidad para mantener el principio del mínimo privilegio.

Principales beneficios para los organismos

- **Favorece el principio del mínimo privilegio:** los usuarios sólo acceden a la información y recursos imprescindibles para el desempeño de su actividad.
- **Favorece el enfoque Zero Trust:** establece un marco de seguridad corporativa en el que sólo usuarios y dispositivos autenticados y autorizados pueden acceder a la información corporativa.
- **Ejerce controles de aseguramiento para superficie de ataque:** asegura la conexión remota mediante cifrado y los dispositivos de usuario.
- **Reduce el riesgo asociado al dispositivo de usuario:** permite la evaluación de postura de dispositivos, estableciendo el cumplimiento de los requisitos mínimos de conexión a la hora de acceder a la red.
- **Mitiga el riesgo de suplantación de identidad:** añade un nivel de seguridad extra mediante doble factor de autenticación.
- **Asistir en la identificación de comportamientos anómalos:** Permite monitorizar todo el tráfico entre el usuario (dispositivo remoto) y el sistema (protocolos usados, datos mandados / recibidos, servicios utilizados, hosts contactados etc.)