PLEC DE PRESCRIPCIONS TÈCNIQUES (PPT) PER A L'ADJUDICACIÓ DEL CONTRACTE DE SUBMINISTRAMENT, CONFIGURACIÓ I POSADA EN FUNCIONAMENT D'UNA SOLUCIÓ CORPORATIVA DE SEGON FACTOR D'AUTENTICACIÓ (2FA)

INTRODUCCIÓ

La xarxa corporativa de Barcelona Activa requereix millorar el seu control d'accés a productes i actius digitals estenent les funcionalitats d'un segon factor d'autenticació, que, actualment està limitat a un entorn intern d'administració. Aquesta solució de segon factor d'autenticació està basada en el producte **FortiAuthenticator**, del fabricant **Fortinet**.

Amb aquesta contractació es vol:

1.) Adquirir les llicències i infraestructures necessàries per ampliar l'actual entorn de 2FA per tal de fer-lo funcional per a tots els usuaris corporatius (interns i externs) i per a totes les xarxes internes i externes així com el seu manteniment pels propers 3 anys.

2.) Contractar tots els serveis professionals necessaris per tal de configurar els diferents entorns, equips de xarxa i de seguretat, així com els diferents elements informàtics (pc's i telèfons mòbils) per tal d'estendre la solució actual a tots els usuaris i entorns corporatius.

CONDICIONS TÈCNIQUES GENERALS

Donat l'abast del projecte i la criticitat de les aplicacions cal tenir en compte les següents premisses:

- Els serveis oferts per dur a terme aquest projecte hauran de tenir en compte que cal actuar sobre sistemes que estan en producció i que ja contenen dades. Per això caldrà que les accions crítiques es realitzin fora d'hores, planificant-ne l'impacte mínim de l'aturada i que es prenguin les màximes precaucions durant la manipulació, tant de maquinari com de dades.

- Caldrà preveure el màxim nivell de serveis professionals que assegurin la correcta implantació i posada en funcionament del sistema així com una resposta ràpida i eficaç davant qualsevol eventualitat, error o anomalia.

- L'oferta haurà d'incloure el manteniment durant 3 anys de tot el material (programari i maquinari) subministrat en el marc del present contracte. Aquesta condició caldrà complir-la amb la garantia del fabricant o amb un contracte de manteniment específic si fos el cas.

L'extensió de la solució actual de 2FA haurà de complir les condicions següents:

- Autenticació centralitzada d'usuaris i ordinadors.

- Integració amb autenticació de doble factor.

- Gestió d'usuaris invitats (tokens temporals).

- Gestió d'onboarding de dispositius de xarxa corporativa.

La solució ha de ser capaç d'intercanviar informació d'usuaris emprant diferents mètodes:

- Integrant-se amb els controladors de Directori Actiu o LDAP per demanar els grups a què pertanyi un usuari.

- Utilitzant un agent propi de single-sign on (SSO) que detecti el login/logout d'usuaris i l'adreça ip associada.

- Autenticació basada en portals, capaç d'integrar-se amb la resta de fonts d'identificació o fins i tot amb xarxes socials.

- RADIUS externs, monitoritzant els paquets d'accounting que contenen informació de l'usuari.

Per facilitar l'operativitat i intentar impactar el mínim possible en la productivitat cal disposar de mecanismes que permetin a l'arquitectura de seguretat reutilitzar les credencials que l'usuari ha fet servir en un sistema d'altres, evitant que hagi d'introduir reiteradament la mateixa informació conforme vagi accedint a diferents recursos.

El sistema de gestió d'identitats sol·licitat ha de facilitar el desplegament d'arquitectures de single sign-on (SSO) multiservei, afegint-hi un rang més gran de mètodes d'autenticació i incrementant l'escalabilitat.

Aquesta plataforma serà, en definitiva, emprada com a garantia de l'accés segur a la xarxa, identificant als usuaris, preguntant a altres sistemes quins permisos tenen i comunicant aquesta informació a altres sistemes, com poden ser firewalls per emprar aquesta informació en polítiques de seguretat basades en identitat.

Es descriuen a continuació amb més detall algunes de les capacitats requerides per a la plataforma de gestió d'identitats:

- Serveis d'autenticació
  - Ha de poder exercir els rols tant de servidor d'autenticació, com de client d'altres repositoris o fonts d'identitat.
  - Ha de poder operar com un servidor de RADIUS i TACACS+ autònom, oferint autenticació tant basada en certificats com no basada en aquests, com EAP-TLS, EAP-TTLS, PEAP, EAP-GTC, i també autenticació MAC per a entorns amb MAB (MacAuthentication -Bypass). Ha de permetre securitzar les connexions RADIUS mitjançant l'ús de RADSec (RADIUS sobre TLS).
  - Ha de poder connectar-se a un servei LDAP (Microsoft Active Directory, OpenLDAP/Gsuite o novel eDirectory) per demanar validar usuaris, per exemple quan rep una petició RADIUS.
  - Ha de poder integrar-se amb l'AD de Windows, almenys per permetre verificar que una màquina intentant accedir a la xarxa hagi estat registrada i contingui credencials vàlides, fent una autenticació de màquina anterior a l'autenticació basada en usuari.
  - Ha de ser compatible amb la solució de VDI de VMWare (Horizon)
  - Ha de ser compatible amb el client VPN Palo Alto (Global Protect)
  - Ha de permetre desplegar portals d'autenticació explícita per a una autenticació manual, per exemple per a casos d'ús com la gestió de convidats (on l'usuari ni tan sols pertany a l'organització).
  - Ha de ser compatible amb OAUTH per integrar l'autenticació amb xarxes socials (almenys Facebook, Google, Linkedin, Twiter), Azure Directory i G-Suite.

- Single Sign on (SSO)
  - Ha de disposar de la capacitat d'integrar-se amb altres serveis d'autenticació disponibles a la xarxa corporativa, per tal d'assegurar que cada usuari només s'ha d'autenticar una vegada, i aquesta autenticació es reutilitzi a la resta de sistemes.
  - Ha de poder detectar quins usuaris han fet login al Directori Actiu, així com permetre integracions via syslog, NTLM, i SAML (tant en rol de Service Provider [SP] com a Identity Provider [IdP]).

- Doble factor d'autenticació
  - Ha de proporcionar una solució de doble factor d'autenticació segura que només els usuaris autoritzats tinguin accés a la informació sensible, aportant una capa addicional de seguretat que redueix dràsticament la possibilitat que es produeixi una pèrdua d'informació.
  - L´ús d´aquest segon factor serà molt ampli, abastant tant l´autenticació dels accessos remots via VPN, com l´autenticació en aplicacions i portals, podent incorporar-se també a l´administració de sistemes i plataformes de seguretat crítics.
  - La plataforma sol·licitada ha de suportar diferents tipus de Token concurrents, tant físics com virtuals, a més de doble factor basat en correu electrònic i SMS.
  - Per facilitar la gestió d'usuaris ha d'incloure portals d'autoregistre, autoprovisionament de tokens i recuperació de contrasenyes.

- Token
  - Es requereix la provisió d'una solució d'OTP (One Time Password) o Token per a 200 usuaris.

- Ha de proporcionar-se en format d'aplicació per a mòbil (compatible amb els sistemes Android, iOS i Windows Mobile), i cal que en un futur es pugui disposar de tokens físics (en format targeta de crèdit/visita o clau USB) per a alguns casos particulars.
- Ha de suportar notificacions push, és a dir, que l'usuari només hagi de prémer per acceptar l'autenticació i que el token sigui enviat automàticament a la plataforma de gestió d'identitats, simplificant la interacció entre el sistema d'autenticació i l'usuari, sense necessitat que sigui l'usuari qui introdueixi els dígits un a un.
- Aquesta solució no ha de requerir cap suport recurrent, sinó aquesta llicència ha de ser perpètua.

- Gestió de certificats
  - La plataforma ha de permetre gestionar el cicle de vida dels certificats corporatius, actuant com a Autoritat de Certificació per crear i signar certificats X.509, tant per a servidors com a clients, incloent serveis propis de PKI's tradicionals com SCEP, CRL's i OCSP.
  - L'ús d'aquests certificats estarà orientat principalment a l'autenticació d'usuaris i servidors, per a accessos remots per VPN, o bé a servidors i serveis web, per exemple.

CONDICIONS TÈCNIQUES PARTICULARS

La solució corporativa de 2FA a Barcelona Activa ha de complir les condicions següents:

1.) L'entorn ha de ser redundat, de forma que l'entorn de 2FA no s'hagi d'aturar mai ni en cas d'avaria ni per processos d'actualització. El funcionament de l'entorn haurà de ser actiu/passiu virtualitzat.

2.) Ha de permetre la integració dels següents entorns:
   a. Directori actiu (ordinadors corporatius)
   b. Azure (Office365)
   c. VDI de VMWare
   d. Wifi Fortinet
   e. VPN Palo Alto

3.) Ha de permetre accedir a un doble factor d'autenticació via token físic i token virtual (aplicació mòbil)

4.) Ha d'estar llicenciat per un mínim de 4.000 usuaris amb una llicència perpètua

Com que en l'actualitat ja es compta amb una llicència corporativa de **FortiAuthenticator**, els ítems que es necessita que se subministrin en aquest contracte per tal de complir aquestes condicions són els següents:

Part Number	Product Description	
Hardware		
FAC-VM-BASE	VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License. Unlimited vCPU. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0, and Xen Virtual Machine platforms	
FAC-VM-1000-UG	FortiAuthenticator-VM 1000 users license upgrade	
FC3-10-0ACVM-248-02-36	FortiCare Premium Support (1 - 5100 USERS)	
FTM-ELIC-1000	Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 1000 users. Electronic license certificate.	
FTK-200B-200	Two Hundred pieces one-time password token, time based password generator. Perpetual license, Compatible with FortiGate, FortiAuthenticator and FortiToken Cloud.Encrypted seed file is available via customer support request.	

SERVEIS

Tal i com s'ha comentat en apartats anteriors, la posada en producció d'aquesta solució passa a ser un element crític per la disponibilitat dels serveis de Barcelona Activa. Un error o mal funcionament de l'eina impedirà l'accés a tots els usuaris corporatius a tot l'entorn digital. Per això proposem el següent calendari d'implementació, pel qual caldrà proposar els serveis necessaris per evitar un impacte a l'entorn de producció corporatiu.

Fase 0: Definició de configuració

Valorar conjuntament amb l'empresa adjudicatària, el responsable de sistemes i el responsable de seguretat quines polítiques de configuració s'ajusten a les necessitats de l'entitat per garantir la seguretat de l'eina mantenint en nivells acceptables l'afectació al servei. Alguns exemples de decisions a valorar poden ser:

- Accions condicionades a IP's d'origen de peticions
- Durada dels tokens en cache
- Segregació de funcions d'administració

Accions a realitzar:

- Barcelona Activa: proporcionar necessitats a cobrir a l'empresa adjudicatària.
- Empresa adjudicatària: proposar opcions de configuració que permetin l'explotació òptima de l'eina segons les necessitats transmeses.

Fase 1: Desplegament de FortiAuth i formació al personal tècnic

Els objectius a assolir en aquesta fase són:

- Desplegament de les instancies de FortiAuth
  - Configuració seguint totes les recomanacions i "best practices" de seguretat: es requerirà la documentació per garantir que la configuració és l'adient.
  - Configuració de la sortida de correus electrònics : caldrà valorar si fer servir connector contra Exchange o Axigen.
- Configuració de l'alta disponibilitat.
- Sincronització amb Active Directori (un domini – CORPORATIU – i una unitat organitzativa).
- Programació de l'assignació de tokens automatitzada durant l'alta i la desasignació en cas de baixa.
- Configuració del FortiAgent a nivell de servidor per preparar el desplegament en endpoint.
  - Cache de tokens.
  - Secret de vinculació FortiAgent.
- Publicació a internet del sistema.
- Primera formació als tècnics sobre l'ús i la gestió de l'eina.
- Proves de funcionament amb endpoints fora de producció.

Aquesta fase no afecta a l'entorn de producció, pel que no és necessari preparar un procediment de rollback.

Accions a realitzar:

- Barcelona Activa:
  - Proporcionar informació necessària pel desplegament i configuració de l'eina.
  - Preparar la infraestructura de xarxa per la publicació de la solució.
  - Configurar el connector d'Azure pel servei SMTP.
  - Traslladar la documentació d'ús a manual per usuaris.
  - Proves de funcionament amb endpoints.

- Empresa adjudicatària:
  - Configurar l'eina segons best practices de seguretat.
  - Configurar l'alta disponibilitat de l'eina.
  - Configurar la sincronització de l'eina amb el domini.
  - Definir la configuració de l'agent.
  - Formar als tècnics en l'ús de l'eina.
  - Generar documentació d'ús.

- Supervisar el resultat de les proves de funcionament.

Fase 2: Distribució de tokens pel personal intern i configuració dels endpoints corporatius

El primer pas serà la distribució dels tokens al personal intern de l'entitat ja que no es podrà començar a desplegar el control si prèviament tots els usuaris no disposen d'un token correctament configurat.
- En el cas de tokens físics, es valora lliurar-los en el moment de la configuració del FortiAgent en l'endpoint.
- Per tokens APP, l'empresa adjudicatària haurà de proposar opcions de distribució massiva centralitzada, que poden ser mitjançant l'ús d'un correu electrònic amb un QR per vincular el token a la APP.

Una vegada garantit que el servidor està correctament configurat i respon a les peticions dels agents caldrà començar el desplegament de la manera menys intrusiva possible.

Donat que l'entorn més controlat és el dels usuaris corporatius, la primera fase suposarà la instal·lació del FortiAgent en portàtils corporatius tal d'implementar el doble factor a nivell d'endpoint. Donat que aquest canvi és crític i s'ha de garantir que l'usuari té, entén i sap fer servir el MFA, convé un desplegament controlat. El procediment temptatiu podria articular-se a partir d'una visita presencial a la Direcció de Tecnologia per tal de:
- Instal·lar l'agent i validar que l'usuari té ben configurat el token
- Realitzar una prova d'inici de sessió
- Recordar l'accés al manual d'usuari del MFA

Un cop es finalitzi amb la configuració dels dispositius personals, caldrà aplicar el FortiAgent als dispositius corporatius compartits que puguin quedar en producció. Tanmateix caldrà modificar la plantilla corporativa per incloure el FortiAgent.

En aquest punt és crític que l'empresa empresa adjudicatària plantegi un sistema de rollback, ja sigui mitjançant una plantilla administrativa per GPO, un control de l'aplicació per SCCM o INTUNE s'ha de poder modificar la configuració de l'agent de manera centralitzada en cas d'error per evitar que un mal funcionament impliqui que tots els usuaris hagin de tornar amb el portàtil a Seu Central per modificar configuracions i poder accedir als EndPoints.

Accions a realitzar:
- Barcelona Activa:
  - Configurar els agents als endpoints i validar l'ús del token per part dels usuaris.
  - Modificar la plantilla corporativa per afegir l'agent.

- Empresa adjudicatària:
  - Configurar el desplegament i enviament de tokens virtuals.
  - Preparar una solució de rollback centralitzada.
  - Supervisar la distribució i solucionar possibles incidències.

Fase 3: Distribució de tokens a personal extern

Es pot valorar si fer aquesta distribució simultàniament que amb els tokens APP per a personal corporatiu o bé esperar a validar que el sistema MFA funcioni amb el personal corporatiu per començar a enviar els tokens al personal extern. En aquests casos el token servirà exclusivament per accedir a la VPN i a l'entorn de VDI.

Tot i que en aquesta fase no es valora necessari un procés de rollback, si que es considera imprescindible una bona campanya de comunicació sobre les característiques i ús de la solució, així com la informació del dia en que començarà a aplicar.

Accions a realitzar:
- Barcelona Activa:
  - Supervisar el desplegament.

- Empresa adjudicatària:
  - Desplegar l'enviament de tokens virtuals a personal extern.

Fase 4: Vinculació amb Office365 i VDI Horizon

La primera cosa que caldrà per abordar aquesta fase és definir un procés de rollback, que en aquest cas serà crític per si cal tirar enrere. Una vegada confirmat que l'entorn funciona en local i que tots els usuaris saben utilitzar correctament els tokens s'ha de procedir a federar el login del SSO d'Azure al FortiAuthenticator. Aquest punt és crític, ja que un error impedirà que tota l'entitat pugui accedir a les solucions O365.

Si es valida que el login s'ha federat correctament i que les aplicacions vinculades al SSO autentifiquen correctament llavors caldrà modificar el sistema SAML d'Horizon i vincular-lo a Azure.

Accions a realitzar:
- Barcelona Activa:
  - Proves de funcionament

- Empresa adjudicatària:
  - Federar el login d'Azure contra la solució de MFA
  - Vincular l'inici de sessió d'Horizon contra Azure
  - Tenir preparat un pla de rollback en cas de problemes

Fase 5: Vinculació amb Global Protect

Arribats a aquesta última fase, caldrà modificar l'accés remot més important a la xarxa corporativa, que és l'accés VPN a través de Global Protect de Palo Alto. Per tal de no interferir en l'entorn de producció, valorem que aquesta intervenció caldria fer-la durant una finestra de cap de setmana per tal de garantir temps de maniobra sense interferir en l'accés dels usuaris corporatius al sistema.

En aquest cas també serà necessari que l'empresa adjudicatària proposi un procés de rollback que ens permeti tirar enrere en cas de fallar l'operació.

Accions a realitzar:
- Barcelona Activa:
  - Supervisar la implementació
  - Proves de correcte funcionament

- Empresa adjudicatària:
  - Modificar la configuració del portal de Global Protect al Firewall perimetral (Palo Alto) per tal de vincular l'inici de sessió.

Marc Puente Vila-Masana
Director de Tecnologia