VZDÁLENÝ PŘÍSTUP

ZAJIŠTĚNÍ BEZPEČNÉHO PŘÍSTUPU K APLIKACÍM A SLUŽBÁM

S ROSTOUCÍMI POŽADAVKY NA MOBILITU A PRODUKTIVITU UŽIVATELŮ JE TŘEBA ZAJISTIT PŘÍSTUP K POŽADOVANÝM APLIKACÍM NEBO SLUŽBÁM PŘI ZACHOVÁNÍ DEFINOVANÉ ÚROVNĚ ZABEZPEČENÍ ZPRACOVANÝCH INFORMACÍ.

Požadavky na dostupnost informací se s postupující elektronizací agend a procesů a s rostoucí mobilitou uživatelů neustále zvyšují. Tlak na zvyšování rychlosti a produktivity při požadavcích na snižování nákladů musí být vyvážen pořízením moderních a bezpečných technologií a jejich správným používáním.
Organizace využívají stále více aplikací a informačních systémů. Tyto aplikace jsou většinou provozovány v interní síti organizace, v rostoucí míře ale využívají i IS vzdálené, hostované u poskytovatelů nebo partnerů, kdy dochází k vytváření tzv. extranetů.
V situaci, kdy má organizace zajistit přístup k interně provozovaným aplikacím či službám, nebo je nutné poskytnout externím partnerům přístup ke správě jimi dodaných řešení, je třeba vyřešit komu, za jakých podmínek a jakým způsobem bude tento přístup poskytnut.

VLASTNOSTI A VÝHODY

- Zajištění bezpečného způsobu přístupu k interním informacím organizace
- Monžnost zajištění preautentizace na rozhraní sítí a auditingu přístupů
- Jednotná autentizace a autorizace uživatelů při přístupu k síťovým službám
- Publikování služeb a aplikací do Internetu při zajištění vysoké dostupnosti

[PUBLIKOVÁNÍ APLIKACÍ]

Požadavky na publikování aplikací a jejich zpřístupnění do Internetu závisí na architektuře aplikace. V základním scénáři, kdy jsou všechny vrstvy aplikace umístěny v interním datovém centru, je třeba vyřešit zejména:

- Vysokou dostupnost všech komponent aplikace a síťového spojení včetně případného vyvažování zátěže
- Způsob autentizace a autorizace přistupujících uživatelů
- Ochranu proti síťovým útokům a kybernetických hrozbám jak na síťové, tak na aplikační úrovni

Autentizace a autorizace

Použití správné metody a způsobu autentizace je spolu s místem její realizace v síťové architektuře určujícím prvkem bezpečnosti na rozhraní sítí a při přístupu k chráněným informacím. Po úspěšné autentizaci je pak zajišťována autorizace na úrovni aplikačních rolí nejlépe jejich integrací s adresářovou službou.
Jedním z důležitých opatření pro eliminaci útoku proti uživatelským heslům je použití dvoufaktorové autentizace, kdy se ideálně používá čipová kata nebo OTP. Pokud tyto způsoby autentizace není možné použít, je vhodné doplnit autentizaci uživatelským jménem a heslem po autentizaci uživatelským certifikátem.
V závislosti na celkové koncepci správy identit v organizaci lze pro správu externích identit použít dedikovanou instanci adresářové služby.
V případě extranetů je možné zajistit federaci identit.

[VZDÁLENÝ PŘÍSTUP DO SÍTĚ]

Je možné, že čelíte požadavkům na zřízení přístupu do interní sítě organizace, a to jak pro interní zaměstnance, tak například i pro externí spolupracovníky nebo dodavatele. Pro tyto případy organizace obvykle provozují VPN přístup. Ten je ale často zbytečný a navíc umožňuje přímou konektivitu na úrovni IP protokolu, která zvyšuje bezpečnostní rizika zejména v situaci, kdy se připojuje do sítě organizace nespravovaný počítač.
Vhodným řešením požadavků na rozsáhlejší přístup do interní sítě organizace je publikování přístupu na vzdálenou plochu.

Vzdálená plocha

Pomocí služeb vzdálené plochy je možné zajistit bezpečný přístup k jednotlivým aplikacím anebo k ploše terminálového serveru či k pracovní stanici uživatele ve vnitřní síti organizace. Správné nasazení služeb vzdálené plochy zajišťuje tyto výhody:

- Dvoufaktorová autentizace uživatele, včetně použití čipových karet
- Přístup pouze k definovaným aplikacím nebo systémům na základě autentizace a autorizace uživatele
- Bezpečnostní kontrola přistupujícího zařízení/počítače a zajištění shody konfigurace s bezpečnostní politikou organizace
- Autentizace serveru vzdálené plochy certifikátem při sestavování připojení
- Zašifrovaná komunikace mezi přistupujícím počítačem a bránou vzdálené plochy

Velkou bezpečnostní výhodou řešení přístupu k aplikacím nebo systémům pomocí vzdálené plochy je, že není vytvořeno propojení přistupujícího počítače a serveru vzdálené plochy na úrovni protokolu IP.

[TECHNOLOGIE VZDÁLENÉHO PŘÍSTUPU]

Služby vzdálené plochy využívají technologií Microsoft Remote Desktop Services. Jedná se zejména o následující role Windows Serveru:

- Remote Desktop Session Host je základní komponentou, která umožňuje přístup ke vzdálené ploše nebo k publikovaným aplikacím pomocí protokolu RDP (Remote Desktop Protocol). Pro připojení se na straně klienta používá aplikace Připojení ke vzdálené ploše (Remote Desktop Connection)
- Remote Desktop Connection Broker, která sleduje uživatelská připojení v load-balancované farmě Remote Desktop Session Host serverů
- Remote Desktop Gateway
- Remote Desktop Licensing, která spravuje přístupové licence RDS CAL, vyžadované pro každé zařízení nebo uživatele přistupující k Remote Desktop Session Host serveru. Remote Desktop Licensing instaluje, vydává a sleduje dostupnost RDS CAL licencí v případě, že jsou licence potřeba.

Remote Desktop Connection Broker

Remote Desktop Connection Broker obsahuje databázi, ve které jsou uloženy informace o připojení uživatele, jako je ID připojení, uživatelské jméno, jméno serveru, ke kterému je uživatel připojen a stav připojení. Při ztrátě spojení se serverem umožňuje Remote Desktop Connection Broker přesměrování navazovaného připojení na Remote Desktop Session Host server, od kterého byl uživatel odpojen. Tím dojde z pohledu uživatele k obnovení stavu vzdálené plochy nebo vzdálené aplikace, nesníží se produktivita práce a nedojde ke ztrátě dat při výpadku spojení mezi klientským počítačem a serverem vzdálené plochy. Remote Desktop Connection Broker také provádí vyvažování zátěže pro nové připojení mezi Remote Desktop Session Host servery, které jsou konfigurovány pro používání Remote Desktop Connection Brokeru. Toto vyvažování zátěže je prováděno na základě aktuálního počtu připojených uživatelů a tím se zvyšuje propustnost řešení.

Remote Desktop Gateway

Remote Desktop Gateway poskytuje komplexní model konfigurace zabezpečení, který řídí přístup ke konkrétním interním síťovým prostředkům. Poskytuje připojení protokolu RDP typu point-to-point, neumožňuje tedy vzdáleným uživatelům přístup ke všem síťovým prostředkům. Umožňuje konfigurovat jak zásady podmínek definujících ověřování, které musí být splněny, aby se vzdálení uživatelé mohli připojit k interním síťovým prostředkům, tak i používání architektury NAP (Network Access Protection) za účelem zdokonalení zabezpečení. Dále poskytuje nástroje pro monitorování stavu a událostí Remote Desktop Gateway.

[BEZPEČNOSTNÍ KONFIGURACE]

Bezpečnostní konfigurace služeb vzdálené plochy je zajišťována pomocí:

- Skupinových politik
- PKI infrastruktury
- Procesu správy aktualizací

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz