BalaBit Shell Control Box 3 F5

A magas jogosultságú felhasználók felügyeletének forradalmi eszköze

- Központosított hitelesítés és hozzáférés-vezérlés
- Munkavállalók és partnerek szorosabb felügyelete
- Gyorsabb és jobb minőségű auditok
- Az IT-s munkatársak szigorúbb elszámoltathatósága
- Alacsonyabb hibaelhárítási és felderítési (forensics) költségek
- Fokozottabb törvényi és iparági megfelelés
- Humán biztonsági kockázatok csökkentése

A 3 F5 verzió újdonságai

- Meglátogatott weblapok képének megtekintése a HTTP(s)-kapcsolatok auditálása közben
- Valós idejű tartalomfelügyelet, riasztás és blokkolás RDP-, VNC- és Telnet-kapcsolatokban
- Integráció más gyártók jelszókezelő rendszerivel
- Erős, tanúsítványalapú hitelesítés az SCB webes felületének eléréséhez

A magas jogosultságú felhasználók korlátlan „hatalma”

Egy cég különböző szervezeti egységeinek felhasználói elérhetik és módosíthatják a cég érzékeny adatait, például a pénzügyi és az ügyfélkapcsolati adatokat, a személyzeti rekordokat vagy a bankkártyaszámokat. Ezen felhasználók között a jogi osztály munkatársaitól kezdve a humánerőforrás-menedzsereken keresztül a számviteli és ügyfélszolgálati munkatársakig számos szerepkör képviselője megtalálható. Ezen privilegizált jogosultságú munkatársak mellett más korlátlan jogú felhasználók (például rendszergazdák, IT-alvállalkozók, vezetők stb.) is vannak a rendszerben, akik gyakorlatilag teljes hozzáféréssel rendelkeznek a cég információvagyona és IT-eszközei felett. E felhasználók tevékenységének szabályozása a hagyományos módszerekkel (még naplózással és írott céges szabályzatokkal is) igen nehéz. Gyakorlatilag lehetetlen megválaszolni a kérdést, hogy ki mit csinált, és az ilyen helyzetek gyakran vádaskodásba torkollnak, miközben az ügyek kivizsgálására rengeteg felesleges pénz és idő megy el.

Független és transzparens auditeszköz

A független auditeszközként működő Shell Control Box (SCB) a magas jogosultságú felhasználók munkameneteinek ellenőrzésével megoldja a fenti problémákat. A Shell Control Box (SCB) tevékenységmonitorozó eszköz szabályozza a távoli szerverek és hálózati eszközök privilegizált felhasználók általi elérését, és nyilvántartást vezet az általuk végzett tevékenységekről. Az így készülő auditnapló nemcsak kereshető, de a tevékenységek filmszerűen is visszajátszhatók. A meglévő IT-környezet ehhez nem igényel módosítást, és az IT-csapat is a megszokott módon folytathatja napi munkáját.

“VIZSGÁLATAINK SORÁN ARRA JUTOTTUNK, HOGY A BALABIT SCB AZ EGYETLEN OLYAN KOMOLY TERMÉK A PIACON, AMI KÉPES AZ SSH-KAPCSOLATOK BIZTONSÁGOS MONITOROZÁSÁRA” - *Øyvind Gielink, biztonsági szakértő, Telenor Group*

westcoast labs
PERFORMANCE VALIDATED

Supported protocols

- HTTP/HTTPS
- Citrix ICA
- VMware View
- VNC
- Telnet/TN3270
- SCP/SFTP
- X11
- TS Gateway
- SSH
- RDP

Központosított hitelesítés

A központosított hitelesítési átjáróként funkcionáló SCB csak erős hitelesítés után engedélyezi a felhasználóknak a kritikus IT-erőforrások elérését. Az SCB felhasználói címtárakkal (például Microsoft Active Directoryval) is integrálható, hogy a védett szerverekhez kapcsolódó felhasználók csoporttagságát lekérdezze. Az SCB a szerverek eléréséhez szükséges hitelesítő adatokat a felhasználót megszemélyesítve, felhasználói beavatkozás nélkül tölti be helyi tanúsítványtárából vagy egy külső jelszókezelő rendszerből. Az automatikus jelszóbeolvasás azért kulcsfontosságú, mert védi a jelszavakat: a felhasználók ugyanis sosem férnek hozzájuk.

Kiemelt tevékenységek felügyelete az SCB-vel

Kifinomult hozzáférés-szabályozás

Az SCB révén egyetlen megoldással elláthatja az elterjedt protokollokon zajló hozzáférések szabályozását és auditálását. A kifinomult hozzáférés-kezeléssel pontosan szabályozhatja, hogy ki, mikor és mit érhet el a szervereken. Emellett a protokollok saját funkcióit és beállításait is szabályozhatja; megadható például az engedélyezett csatornák típusa. Letilthatja például a szükségtelen csatornákat, úgymint a fájlátviteli és fájlmegosztási csatornákat, ezzel is csökkentve a szerverek biztonsági kockázatát. Az SCB-vel egyetlen rendszer elegendő a hozzáférési szabályok betartatásához, ez pedig magas fokú biztonságot garantál a teljes infrastruktúrában – minimális költségek mellett.

4-eyes típusú (kétrésztvevős) engedélyezés

A nem szándékos félrekonfigurálás és más emberi hibák elkerülésére az SCB támogatja a 4-eyes néven ismert engedélyezési sémát, aminek révén egy felügyelő engedélyéhez köthető az adminisztrátor hozzáférése a szerverhez. A felügyelőnek lehetősége van az adminisztrátor munkájának valós idejű követésére is, mintha ugyanazt a képernyőt néznék.

Valós idejű védelem a kártékony tevékenységek ellen

Az SCB-vel valós időben felügyelhető a hálózati forgalom, és különböző műveletek indíthatók a képernyőn megjelenő gyanús minták (például gyanús parancs, ablakcím vagy szöveg) esetén. Az SCB a számok, például a bankkártyaszámok felismerésére is alkalmas. A gyanús felhasználói tevékenységek észlelésekor az SCB e-mailbeli riasztást tud küldeni, de akár azonnal meg is szakíthatja a felhasználó kapcsolatát. Az SCB képes például arra, hogy még azelőtt blokkoljon egy kapcsolatot, mielőtt egy veszélyes rendszergazdai parancsot végrehajtanak a szerveren.

Magas minőségű audit és forensics

Az SCB minden felhasználói tevékenységet visszakövethetővé tesz a tevékenységek magas minőségű, manipulációvédett és megbízható auditnaplókba rögzítésével. Az SCB képes a naplózott tevékenységek filmszerű visszajátszására, amiben a felhasználók minden lépése pontosan úgy látszik, ahogy azt ők látták a saját képernyőjükön. Az Audit Playerrel módosíthatja a lejátszás sebességét, továbbá eseményekre (például beírt parancsok vagy az Enter lenyomása) és a felhasználó monitorán megjelent szövegekre is kereshet. Problémák esetén (mint egy adatbázis módosítása, váratlan rendszerleállások és így tovább) az esemény körülményei rögtön hozzáférhetőek az auditnaplókban, így az incidens oka egyszerűen megállapítható. Az igény szerint előállítható tevékenységjelentések az auditálási folyamat támogatásának egy újabb lépését jelentik, és az elhárítási lépések alapjául szolgálhatnak. Az SCB összességében egy költséghatékony és a törvényi előírásoknak megfelelő megoldás a belső és külső auditok, illetve incidensek kivizsgálásának támogatására.

Alkalmazási területek

- Szabályozási megfelelés (PCI-DSS, ISO2700x, jogszabályok stb.)
- Rendszergazdák és fejlesztők felügyelete
- Kiszervezett feladatokat végző és felhőinfrastruktúrát szolgáltató partnerek felügyelete
- Citrix és VMware View felhasználók auditálása
- IT- és biztonsági események kivizsgálása (hibaelhárítás és forensics)
- Megfelelés a szigorú biztonsági követelményeket előíró vállalatok szabályzatainak

További információk

- A Shell Control Box weblapja
- Online demó kérése
- Visszahívás kérése

Felhasználók a világ minden részéről

orange, EMPH, CEZ GROUP, SKOLKOVO, interoute, LEEKIE ENTERPRISES, telenor, MTS, bitbrains, Handelsbanken, Raiffeisen, WILO, Dubai Islamic Bank, FIDUCIA IT-Partner