



Oprávnenia

Vitajte v ľudskej stránke vašich bezpečnostných systémov!

V tejto lekcii preskúmame, ako sa nastavujú a spravujú oprávnenia v rámci Systému C4.

Pochopenie týchto princípov nám umožní naplno využívať potenciál C4 na zabezpečenie bezpečnej a efektívnej správy zdrojov.

Používatelia Systému C4 sú často zodpovední len za určité budovy, poschodia, či oddelenia v rámci svojej spoločnosti. Aby mali prístup len k informáciám, na ktoré majú oprávnenie, je potrebné nastaviť oprávnenia individuálne pre každého používateľa.

V oblasti zabezpečenia dát a riadenia prístupu existujú vo všeobecnosti dve hlavné stratégie správy prístupu k informáciám.

Prvou stratégiou je zabezpečenie založené na rolách.

Obmedzuje prístup na základe rolí používateľov v rámci organizácie. Roly sa stanovujú počas fázy navrhovania aplikácie, na základe povinností a potrieb používateľov.

Každá rola má pridelené oprávnenia, ktoré definujú prístup k rôznym častiam systému.

Napríklad, inštalačný manažér má prístup ku všetkým inštaláciám, produktový manažér má prístup ku všetkým produktom a administrátor má prístup ku všetkým dátam.

Táto stratégia sa nazýva aj zabezpečenie na úrovni stĺpca.

Oprávnenia sú priradené k rolám, a používatelia získavajú tieto oprávnenia prostredníctvom svojich rolí.

Tento prístup je jednoduchší na implementáciu a správu, avšak umožňuje menej detailné nastavenie oprávnení.



Preto veľké systémy často používajú koncept zabezpečenia na úrovni záznamu, ktorý riadi prístup k jednotlivým záznamom v rámci systému. Tento prístup sa nazýva aj zabezpečenie na úrovni riadku.

Tento koncept využíva aj Systém C4, ktorý ponúka vysoko dynamické a detailné nastavovanie oprávnení na úrovni riadkov.

Ak máme troch inštalčných manažérov, každý z nich má prideleného iného zákazníka, tak každý manažér môže vidieť len riadky týkajúce sa inštalácií jeho zákazníka.

Zabezpečenie na úrovni záznamu umožňuje veľmi presnú kontrolu nad tým, kto môže pristupovať k určitým riadkom dát v rámci databázy a kto ich môže upravovať.

C4 Systém pre správu oprávnení využíva hierarchickú štruktúru, pričom ide o kombináciu hierarchie typu strom a flat hierarchie typu skupina.

Hierarchia typu strom je multiúrovňová a umožňuje neobmedzený počet vnorení. Každá entita sa nachádza v strome len raz a má len jedného parenta.

Flat hierarchia typu skupina je jednoúrovňová a všetky položky sú v rámci nej rovnocenné.

Podme sa teraz bližšie pozrieť na to, ako sa nastavujú oprávnenia v prostredí Systému C4.

Oprávnenia v Systéme C4 sa spravujú v záložke Permissions.

V prostredí Systému C4 predstavujú oprávnenia vzťah medzi osobou a akýmkoľvek dátovým objektom spravovaným v systéme. Dostupné dátové objekty, na ktoré je možné nastaviť oprávnenia, sa nachádzajú na ľavej strane.

V našej lekcii budeme nastavovanie oprávnení demonštrovať na príklade zariadení.

V stĺpcoch pri každom podsystéme nájdete jednotlivé typy oprávnení ako napr. Vytvoriť, Čítať, Upraviť, či Odstrániť. Počet a typy týchto oprávnení zodpovedajú rozsahu C4, v akom ju používateľ využíva. V prípade potreby je možné v budúcnosti pridať ďalšie oprávnenia.



Každému z týchto typov oprávnenia môžeme prideliť hodnotu Povolit' alebo Zakázať.

Jedným z typov oprávnení je Prístup, avšak pre uľahčenie práce používateľovi je spravovanie prístupových práv vyčlenené do samostatnej záložky. Táto záložka obsahuje len koncové body, na ktorých sa oprávnenia vyhodnocujú (zvyčajne dvere a poplachové oblasti).

Každý typ oprávnenia sa vyhodnocuje samostatne, avšak pri všetkých typoch platia rovnaké princípy. V našej lekcii si tieto princípy vysvetlíme na príklade oprávnenia typu Read.

V nasledujúcich animáciách bude čiara reprezentovať oprávnenie typu Čítať, ktoré priradíme osobe na zariadenie.

Oprávnenia s hodnotou Povolit' sú zobrazené zelenou farbou, zatiaľ čo oprávnenia s hodnotou Zakázať sú zobrazené červenou. Oprávnenia ďalej môžu byť nastavené s dedením alebo bez dedenia.

Podme sa teraz bližšie pozrieť na tieto jednotlivé druhy oprávnení a kombinácie, ktoré môžu vzniknúť.

Základnou možnosťou nastavenia oprávnenia je jeho priame nastavenie na príslušný koncový bod.

Hoci pre zjednodušenie správy oprávnení je vhodné čo najviac využívať hierarchickú štruktúru a dedenie, v prípade potreby je možné nastaviť oprávnenie aj presne na jednu konkrétnu entitu.

Napríklad pridelíme oprávnenie s hodnotou Povolit' priamo na čítačku kariet 102.

Oprávnenia nastavené priamo na entitu platia vždy s najvyššou prioritou, a nie je možné to žiadnym dedením zmeniť.

Takto nastavené oprávnenia sú v Systéme C4 zobrazené v plnej farbe.

Ďalšou možnosťou je nastavenie oprávnenia s dedením. Hierarchický systém, tak ako ho používa C4 umožňuje rýchle vyhodnocovanie dedenia a podporuje neobmedzený počet vnorení.

Vďaka tomu je možné rýchlo a jednoducho nastavovať oprávnenia, ktoré sa automaticky dedia na podriadené entity.



Napríklad, ak nastavíme oprávnenie s dedením s hodnotou Povolit' na ovládací panel 1, zdedí sa aj na všetky dvere a čítačky kariet pod týmto ovládacím panelom.

Zdedené oprávnenia sú v Systéme C4 reprezentované bledou farbou.

Ak chceme povoliť dedenie oprávnenia, ale vynechať určité uzly, pridáme oprávnenie s hodnotou Zakázať na uzly alebo entity, ktoré nechceme povoliť.

Napríklad, ak na ovládacom paneli 1 nastavíme hodnotu Povolit' s dedením, a na dvere 102 nastavíme hodnotu Zakázať s dedením, tak sa hodnota Povolit' aplikuje na všetky podriadené uzly, okrem dverí 102 a čítačky kariet 102.

Pri dedení môže nastať otázka, ktoré oprávnenie má prednosť, keď sú v rámci hierarchickej štruktúry pridelené rôzne oprávnenia.

Napríklad, ovládací panel 1 má hodnotu Povolit' s dedením, a dvere 102 majú hodnotu Zákaz s dedením. Ktorá z týchto hodnôt sa vzťahuje na čítačku kariet 102? Pravidlo je, že vždy má prednosť to oprávnenie, ktoré je najbližšie k uzlu, ktorý vyhodnocujeme. V našom prípade sú najbližším uzlom dvere 102, a preto sa aplikuje hodnota Zakázať.

To isté pravidlo platí aj pri opačnom poradí hodnôt Povolit' a Zakázať. V tomto prípade čítačka kariet 102 zdedí hodnotu Povolit' od dverí 102, ktoré sú najbližším nadradeným uzlom.

Máme tiež možnosť nastaviť aj oprávnenie bez dedenia. Takéto oprávnenie platí len pre ten konkrétny uzol, na ktorý bolo nastavené, a nevzťahuje sa na podriadené uzly.

Napríklad, ak na ovládacom paneli 1 nastavíme hodnotu Povolit' s dedením, ale na dvere 102 nastavíme hodnotu Zakázať bez dedenia, tak pre dvere 102 platí zákaz, zatiaľ čo čítačky kariet ako aj ostatné dvere pod týmto ovládacím panelom budú mať povolenie zdedené od ovládacieho panela.

To isté pravidlo platí aj pre opačné poradie hodnôt Povolit' a Zakázať.

Pre jednoduchšie priradovanie oprávnení Systém C4 umožňuje aj vytváranie tzv. skupín, ktoré si bližšie popíšeme v nasledujúcej časti videa.

Predstavme si situáciu, že fyzické rozloženie podsystémov v budove neumožňuje jednoduché nastavenie oprávnení podľa logických celkov. Chceme napríklad nastaviť oprávnenia na všetky dvere jedného konkrétneho poschodia, avšak tieto



dvere sú ovládané viacerými ovládacími panelmi. Základný strom zariadení nepodporuje takýto druh usporiadania.

Preto Systém C4 umožňuje vytváranie dodatočných logických štruktúr, ktoré sa nazývajú skupiny, a poskytujú nám možnosť usporiadať entity podľa našich potrieb.

Keď chceme nastaviť, aby osoba mala oprávnenie ísť na prvé poschodie, z dverí prvého poschodia vytvoríme skupinu. Umiestnime do nej dvere 101, 102 a 103. Teraz môžeme prideliť osobe oprávnenie na túto skupinu.

Oprávnenia pridelené skupine sa aplikujú aj na príslušné entity v originálnom strome.

Ako naznačuje šípka v dolnom rohu ikoniek, všetky entity v skupine sú referenciami na existujúce entity v originálnom strome. Skupiny nemôžu obsahovať žiadne nové entity.

V rámci skupiny neexistuje hierarchia. Všetky entity sú na rovnakej úrovni. Každý uzol je teda potrebné pridať priamo, nie je možné do skupiny pridať uzol spolu so svojimi childami.

V prípade zariadení sa tieto skupiny nazývajú access levely. Umožňujú logicky združiť zariadenia z rôznych ovládacích panelov tak, aby bolo nastavovanie prístupov jednoduchšie.

Ako sa vypočítavajú oprávnenia pri skupinách?

Predstavte si, akoby bola skupina umiestnená tesne pred entitou, ktorú vyhodnocujeme.

Keď ovládací panel 2 má hodnotu Zakázať, ktorá sa dedí na podradené uzly, ale skupina prvého poschodia má hodnotu Povolíť, na dvere 101 sa aplikuje hodnota Povolíť, pretože skupina je vnímaná ako najbližší uzol k dverám.

Pri skupinách sa odporúča pracovať len s hodnotou Povolíť. Aplikovanie hodnoty Zakázať na skupiny môže výrazne skomplikovať vypočítavanie oprávnení.

Pri určitých zariadeniach je možné vytvoriť špeciálny typ skupiny s názvom poplachová oblasť, ktorá obsahuje detektory. Tieto detektory pritom musia byť riadené rovnakým ovládacím panelom.



Pre takúto skupinu platia rovnaké pravidlá ako pre klasické skupiny, avšak je tu jedna výnimka: poplachová oblasť môže byť umiestnená aj vo vnútri hierarchie stromu, pretože je súčasťou konfigurácie daného zariadenia.

S poznatkami z tejto lekcie ste pripravení nastavovať oprávnenia v Systéme C4 efektívne a podľa vašich potrieb.