Politika řízení přístupu

I. Úvodní ustanovení

1) Politika řízení přístupu stanovuje pravidla pro přístup k sítím, systémům a datům významných informačních systémů (dále také *„VIS"*) a rozpracovává požadavky na kybernetickou bezpečnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také *„zákon o kybernetické bezpečnosti"*) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také *„vyhláška o kybernetické bezpečnosti"*) v podmínkách Univerzity Hradec Králové (dále také *„UHK"*).
2) Účelem politiky řízení přístupu je zajistit, aby k informacím a prostředkům VIS měli přístup pouze oprávnění uživatelé. Pro přístup k těmto prostředkům jsou stanovena pravidla, která určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv.

II. Princip minimálních oprávnění/potřeba znát (*need to know*)

1) Pro všechny typy účtů musí být uplatněn princip need-to-know.
2) Pravidla pro řízení přístupových oprávnění:
   a) Každý uživatel má přístup pouze k těm aktivům, která nezbytně potřebuje k výkonu své pracovní činnosti.
   b) Základní rozsah oprávnění k jednotlivým aktivům je definován jako minimum potřebného pro činnosti, které uživatel potřebuje. Oprávnění jsou členěna do uživatelských rolí. Vedení UHK není výjimkou a má využívat běžné uživatelské účty.
   c) Privilegované účty mají přiděleny samostatné přihlašovací údaje. Jednotliví administrátoři musí mít vedle privilegovaného účtu i účet běžného uživatele pro činnosti, které nevyžadují privilegovaná oprávnění.
   d) Změna rozsahu přístupových oprávnění je řízena aplikačním správcem VIS a schvalována Manažerem KB.

III. Požadavky na řízení přístupu

1) Za řízení přístupu a stanovení pravidel je odpovědný Garant příslušného aktiva.
2) Za stanovení pravidel v oblasti řízení přístupu je odpovědný aplikační správce VIS.
3) Musí existovat evidence všech uživatelských účtů, pomocí které je možné jednoznačně identifikovat osobu používající daný uživatelský účet.
4) Přístupy a pokusy o přístup musí být automaticky zaznamenávány a monitorovány. Záznamy musí být uchovány po dobu minimálně 18 měsíců u systémů provozovaných jako VIS a po dobu minimálně 12 měsíců u ostatních informačních systémů. U uživatelských účtů musí být nastaveno automatické uzamčení obrazovky při nepřítomnosti uživatele. Pro opětovné odemčení musí být vyžadovány autentizační údaje.
5) Autentizační údaje nesmí být sdíleny více osobami.
6) Přidělování přístupových práv se řídí pravidly:
   a) každý prvek informační a komunikační technologie má řízený a dokumentovaný proces přidělování přístupových práv,
   b) je prováděna pravidelná kontrola řízení přístupových práv a stanovených pravidel pro řízení přístupových práv,
   c) přidělování přístupových práv uživatelům je prováděno pouze v rozsahu nutném pro výkon jejich pracovních povinností,
   d) kontrola přidělených přístupových práv je prováděna při každé změně a minimálně jednou za rok,
   e) pro každý prvek informační a komunikační technologie je vedena aktuální evidence všech uživatelských účtů,
   f) pro každý prvek informační a komunikační technologie je definován systém uživatelských rolí a oprávnění,
   g) je vedena evidence o uskutečněných přístupech a o pokusech o přístup k aktivu,
   h) zákaz přístupu k aktivům VIS prostřednictvím veřejných sítí (např. z nechráněné sítě v restauracích apod.),
   i) role uživatelů, privilegovaných uživatelů a bezpečnostních rolí jsou odděleny,
   j) postup řízení přístupů při mimořádných situacích je dokumentován.

IV. Životní cyklus řízení přístupu

1) Řízení přístupů je dokumentováno pro každé aktivum a probíhá ve fázích:
   a) žádost o přidělení přístupových práv,
   b) schvalování a přidělení přístupových práv,
   c) pravidelná kontrola přístupových práv,
   d) změna přístupových práv,
   e) zrušení přístupových práv.
2) V žádosti o přidělení přístupových práv jsou definovány minimálně:
   a) osoba oprávněna žádat,
   b) uživatel,
   c) rozsah oprávnění a jejich zdůvodnění,
   d) doba platnosti oprávnění.
3) V procesu schvalování a přidělení přístupových práv je definován minimálně:
   a) osoby oprávněné schválit požadavek,
   b) schvalovací lhůty,
   c) osoby nastavující příslušná oprávnění.
4) V procesu změny přístupových práv je definována minimálně:
   a) osoba oprávněna žádat,
   b) uživatel,
   c) požadavek na změnu rozsahu oprávnění,
   d) doba platnosti oprávnění,
   e) osoby oprávněné schválit požadavek,
   f) schvalovací lhůty,
   g) osoby nastavující příslušná oprávnění.
5) Ke zrušení přístupových práv k informacím a aktivům dochází:
   a) při ukončení nebo změně pracovního nebo smluvního vztahu nebo výkonu role uživatele,
   b) na základě procesů definovaných v provozní dokumentaci jednotlivého aktiva.
6) Pro řízení životního cyklu řízení přístupů k prostředkům informační a komunikační technologie je primárním nástrojem jednotný Identity management systém (IDM), pomocí kterého probíhá řízení a automatizace celého životního cyklu identit. Zřizovaní účtů s konkrétní úrovní oprávnění u VIS probíhá na základě písemné žádosti. Rušení účtů a přístupových oprávnění probíhá na základě písemné žádosti, odebírání oprávnění a přístupů je řešeno v rámci procesu offboardingu.

V. Řízení privilegovaných oprávnění

1) Privilegovaným oprávněním se rozumí přístupové oprávnění k účtu, které umožnuje v jednotlivém prvku informační a komunikační technologie:
   a) vykonávat činnosti nad rámec běžného uživatele IS,
   b) provádět změny v nastavení IS,
   c) měnit rozsah přidělených oprávnění jednotlivých rolí a uživatelů,
   d) vykonávat servisní činnosti bez přítomnosti uživatele.
2) Pro privilegované oprávnění je přiřazen odlišný identifikátor uživatele od běžně používaného uživatelského účtu.
3) Běžné činnosti nejsou prováděny s použitím privilegovaného oprávnění.
4) Musí být nastaveno časové omezení platnosti přihlašovací relace, po jehož vypršení následuje automatické odhlášení od systému.
5) Privilegovaná oprávnění se poskytují pouze zaměstnancům UHK či dodavatelům, kteří k výkonu své práce nutně potřebují přístup k citlivým zdrojům, a to pouze v nezbytně nutném rozsahu.
6) Privilegovaná oprávnění musí být pravidelně revidována a kontrolována, aby bylo zajištěno, že jsou stále v souladu s principem minimálních oprávnění.
7) Používání privilegovaných oprávnění musí být monitorováno a zaznamenáváno, aby bylo zajištěno, že je používáno v souladu s těmito pravidly.
8) V případě, že dojde k porušení pravidel řízení přístupu privilegovaných oprávnění, může být přístup k privilegovaným oprávněním dočasně omezen nebo zrušen.

VI. Řízení přístupu pro mimořádné situace

1) Za účelem zajištění kontinuity činnosti během kybernetické bezpečnostní události a kybernetického bezpečnostního incidentu nebo jiných mimořádných situací jsou jednorázově nastavena přístupová oprávnění nad rámec standartního režimu provozu prvku informační a komunikační technologie.
2) Rozhodnutí o přidělení mimořádných oprávnění spadá do kompetence Manažera kybernetické bezpečnosti (dále také *„Manažer KB"*), takové rozhodnutí musí být spolu s rozsahem přidělených oprávnění řádně zdokumentováno.
3) Poté, co pominuly důvody udělení mimořádných oprávnění, musí být dosaženo původního stavu a proveden úplný audit oprávnění v rámci VIS.
4) Všechny aktivity účtů, kterým byla přidělena mimořádná oprávnění, budou logovány a logy budou ukládány tak, aby byla vyloučena možnost jejich pozměnění či odstranění.

VII. Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách

1) V rámci správy identit je zaveden proces pravidelné kontroly a revize přidělených oprávnění a jejich využívání, jehož cílem je zajištění trvalého souladu přidělených oprávnění s pracovní činností uživatelů, udržení konzistentního modelu oprávnění, kontroly přístupů ke skupinovým účtům a dalších parametrů přispívajících k zajištění bezpečnosti spravovaných dat a informací.
2) Kontrola a revize přístupových oprávnění v jednom cyklu je provedena na celém rozsahu uživatelských oprávnění.

VIII. Závěrečná ustanovení

Politika řízení přístupu vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

prof. Ing. Kamil Kuča, Ph.D., v. r.
rektor