Politika bezpečnosti komunikační sítě

I. Úvodní ustanovení

1) Politika bezpečnosti komunikační sítě stanovuje způsob ochrany komunikačních sítí 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) Tato politika je závazná pro všechny zaměstnance UHK odpovědné za zajištění bezpečnosti komunikační sítě v rámci UHK.

II. Pravidla a postupy pro zajištění bezpečnosti sítě

1) Komunikační síť je segmentována a logicky oddělena za účelem zajištění bezpečnosti prvků infomačních a komunikačních technologií a odolnosti vůči případným útokům.
2) Každá část komunikační sítě je dokumentovaná ve fyzické a logické vrstvě. Za vedení dokumentace odpovídá Garant podpůrného aktiva.
3) Je stanoven systém řízení komunikace v rámci komunikační sítě a bezpečnostní perimetry. Správa sítě a síťových prvků je oddělena od správy pracovních stanic a serverů.
4) Při použití vzdáleného přístupu (bezdrátová i kabelová komunikace) je zaveden systém šifrování, aby nemohlo dojít k narušení důvěrnosti, dostupnosti a integrity dat.
5) Jsou zavedeny nástroje a způsob detekce nežádoucích událostí, monitoringu komunikace na síti a zaveden proces pro blokování nežádoucí komunikace.
6) Pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty jsou použity nástroje, které zajistí ochranu integrity komunikační sítě.

III. Určení práv a povinností za bezpečný provoz sítě

1) Vedoucí oddělení informačních technologií (dále také *„OIT"*) je odpovědný za:
   a) architekturu komunikační sítě,
   b) nastavení komunikační sítě a správu aktualizací komunikační sítě,
   c) provoz komunikační sítě,
   d) přidělování přístupů do komunikační sítě,
   e) sledování, zaznamenávání a blokování nežádoucí komunikace v komunikační síti a identifikaci síťových zařízení,
   f) efektivní využití všech dostupných bezpečnostních funkcí používaných technologií.
2) Vedoucí OIT dále posuzuje nastavení a změny bezpečnosti provozu sítě a navrhuje opatření k zajištění bezpečného provozu sítě.

IV. Pravidla a postupy pro řízení přístupů v rámci sítě

1) Přístup do sítí je minimalizován tak, aby každý zaměstnanec UHK přistupoval pouze v rozsahu, který je nutný pro výkon jeho pracovních povinností.
2) Pravidla jsou aplikovatelná na všechny komunikační sítě ve správě UHK alespoň v rozsahu:
   a) interní sítě LAN (včetně SAN),
   b) externí sítě WAN,
   c) propojení na externí sítě (Internet).
3) Pravidla pro řízení přístupu jsou aplikována na všechny segmenty sítě LAN.
4) Pro přístupy uživatelů a administrátorů do vnitřní sítě jsou použity nástroje pro správu a ověření identity.
5) Pro přístupy technických prostředků do vnitřní sítě jsou použity nástroje pro správu přístupu technických prostředků.
6) Přístupy jsou řízeny v jednotlivých prvcích informační a komunikační technologie na základě skupin a rolí.
7) O přidělení a odebrání práv jsou vedeny záznamy.

V. Pravidla a postupy pro ochranu vzdáleného přístupu k síti

1) Vzdálený přístup do sítě je omezen pouze na určená zařízení a pro uživatele, kteří jej potřebují pro výkon svých odpovědností a pouze na dobu, která je nutná pro uživatele.
2) Vzdálený přístup uživatelů k sítím je řízen prostřednictvím odpovídajících technických prostředků.
3) Přístup z externích sítí je možný jen do demilitarizovaných zón (DMZ) navržených tak, aby případný vnější útok neohrozil bezpečnost interní sítě.
4) Vzdálený přístup je možný jen prostřednictvím komunikačního kanálu chráněného kryptografickými prostředky.
5) Vzdálené připojení dodavatelů je možné jen na základě oboustranné dohody, jejímž obsahem je povinně vzájemně akceptovaná bezpečnostní politika a výsledky analýzy rizik vyplývající z tohoto připojení.
6) 6. Ověření identity žadatele o vzdálený přístup je provedeno formou vícefaktorové autentizace.

VI. Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

1) Prvky informační a komunikační technologie jsou trvale monitorovány.
2) Záznamy událostí prvků informační a komunikační technologie je nutné uchovávat nejméně po dobu vyžadovanou zvláštním právním předpisem, nejméně však po dobu 12 měsíců.
3) Záznamy událostí jsou zajištěny před neoprávněným přístupem a neoprávněnou modifikací.
4) Všechny prvky informační a komunikační technologie jsou napojeny na určený zdroj přesného času a jsou nejméně jednou za den synchronizovány.

VII. Závěrečná ustanovení

Politika bezpečnosti komunikační sítě vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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