

EUR European
EN Environmental
IC Innovation
A Initiative

ENVIRONEXT ➤

Kybernetická bezpečnost vodohospodářských technologií

Martin Hlavačka
Patrik Milán
Christian Danížek

Prečo je bezpečnosť dôležitá?

Každý technologický systém sa buduje na to, aby bezpečne vykonával svoju úlohu – v našom prípade zabezpečoval zásobovanie vodou, odvádzanie a čistenie odpadových vôd.

Akékoľvek narušenie tejto funkcie považujeme za zásah do bezpečnosti systémov, čo môže mať dôsledky rôzneho rozsahu - zdravotné, technické, technologické, ale aj branno-bezpečnostné.

Aké môžu byť následky?

Zdravotné – v dôsledku nesprávnej či nedostatočnej funkcie technológie znížená kvalita pitnej vody, neúčinná dezinfekcia vody, biologické poškodenie útvarov povrchových alebo podzemných vôd, poškodenie zdravia pracovníkov ČOV.

Technické – poškodenie čerpadiel chodom na sucho, termická deštrukcia motorových vinutí a káblov, zadretie ventilov, tlakové deformácie a prierazy potrubí a nádrží, poškodenie zariadení predávkovaním funkčnými činidlami, zámenou činidiel, neželané zmeny konfiguračných a kalibračných parametrov jednotlivých technologických zariadení.

Aké môžu byť následky?

Technologické – upchatie filtrov, sít a membrán, zanesenie nádrží, dopravníkov a potrubí kalmi, sedimentami, alebo nánosmi. Kontaminácia čistej časti technológie prienikom znečistenej vody.

Branno-bezpečnostné v dôsledku deoxygenácie, alebo priameho úniku biologického kontaminantu, alebo poškodenia technológie znemožnená dodávka pitnej vody veľkého rozsahu, veľkoplošné znečistenie územia či povodia, až po kolaps vodného ekosystému s možnými katastrofálnymi dôsledkami pre obývateľnosť územia.

Analýza rizík – zlomyseľné konanie

Denial of Service / Denial of Control – útočník sa zámerne snaží narušiť normálne fungovanie systému alebo zabrániť prístupu autorizovanej osoby k systému napr. jeho preťažením.

Configuration Poisoning – útočník skryto alebo otvorene zmení konfiguračné alebo kalibračné parametre systému tak, aby spôsobil jeho znefunkčnenie počas bežnej prevádzky

Manipulation of Control – útočník priamo ovláda jednotlivé zariadenia s úmyslom poškodiť samotné zariadenie alebo čistotu vody

Backdoor – získanie skrytého neoprávneného prístupu do systému s cieľom neskoršieho využitia - napr. zhromažďovanie dát
(Cross Access, False Blacklist, False Whitelist)

Analýza rizík – nedostatočná znalosť obsluhy

Nedostatočná **kvalifikácia** pracovníkov obsluhy, ich nedbanlivosť, únava alebo **vyčerpanie** môžu pri otvorených systémoch predstavovať závažné riziko. Vo výnimočných alebo **kritických situáciách** sa môže prejaviť aj **nedostatok skúseností**, nedostatok tréningu alebo tréningových dát.

Nie každý pracovník má rovnakú schopnosť alebo dostatok času porozumieť **komplexnosti technológie**, nie každé pracovisko má zabezpečenú obsluhu 24/7 dostatočne kvalifikovanými pracovníkmi.

Vzniku nebezpečných situácií je potrebné predchádzať **systemovo** a pracovníkom prideľovať právomoci s rôznymi úrovňami oprávnenia.

Analýza rizík – predchádzanie nehodovým situáciám

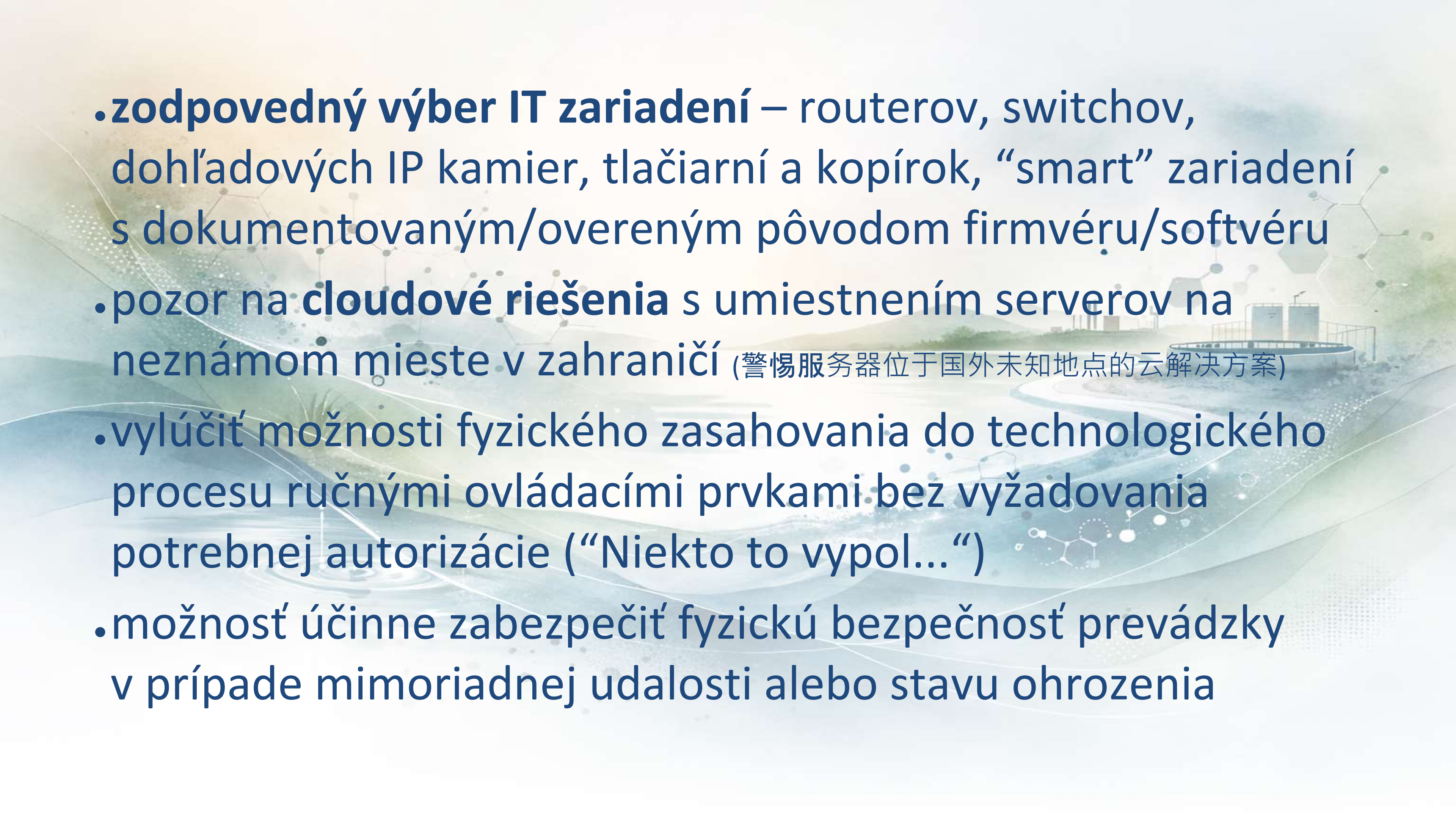
Data Health - samostatnou súčasťou posúdenia bezpečnosti technológie je otázka spoľahlivosti a dôveryhodnosti údajov z meracích zariadení a kontrolných obvodov.

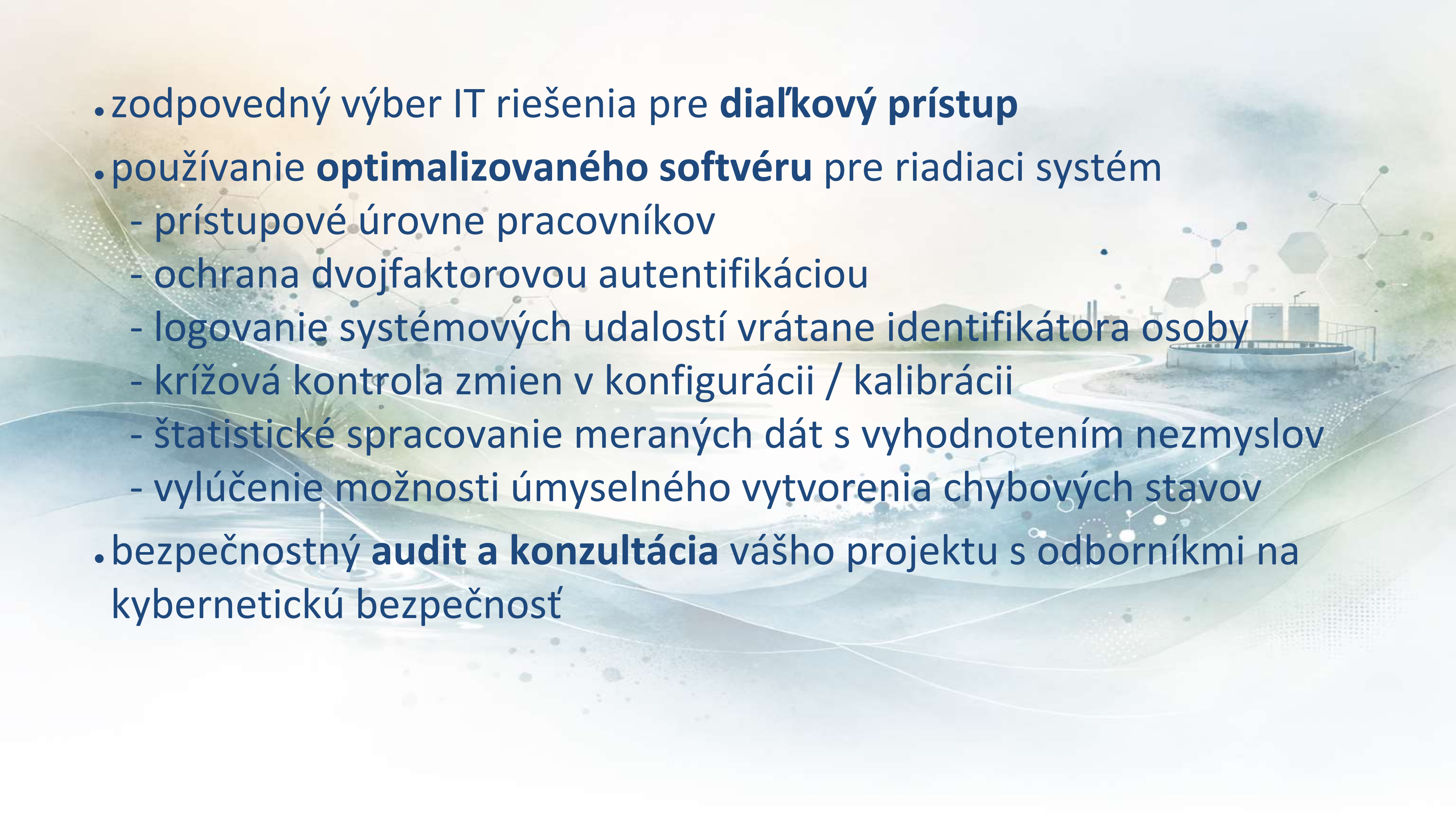
Štatistické vyhodnocovanie meraných dát a priebežná analýza trendov meraných údajov eliminujú budúce chyby spôsobené použitím nesprávnych podkladových dát do rozhodovacieho alebo regulačného procesu.

IT hygiena ako jediná účinná prevencia budúcich rizík

- Určenie stupňov zodpovednosti a úrovni prístupu pre jednotlivých pracovníkov obsluhy
- Zodpovedné pridelovanie osobných hesiel, identifikátorov a kontrola ich správneho používania
- Vyhýbať sa ľahko uhádnuteľným heslám (nbusr123)



- 
- **zodpovedný výber IT zariadení** – routerov, switchov, dohľadových IP kamier, tlačiarňí a kopírok, “smart” zariadení s dokumentovaným/overeným pôvodom firmvéru/softvéru
 - **pozor na cloudové riešenia** s umiestnením serverov na neznámom mieste v zahraničí (警惕服务器位于国外未知地点的云解决方案)
 - **vylúčiť možnosti fyzického zasahovania** do technologického procesu ručnými ovládacími prvkami bez vyžadovania potrebnej autorizácie (“Nieкто to vypol...”)
 - **možnosť účinne zabezpečiť fyzickú bezpečnosť prevádzky** v prípade mimoriadnej udalosti alebo stavu ohrozenia

- 
- The background is a soft-focus, abstract composition. It features several molecular models with blue and green spheres connected by lines, floating in the upper right. Below these, there's a circular, metallic-looking platform or structure. The overall color palette is light blue, green, and white, with a sense of depth and movement.
- zodpovedný výber IT riešenia pre **dial'kový prístup**
 - používanie **optimalizovaného softvéru** pre riadiaci systém
 - prístupové úrovne pracovníkov
 - ochrana dvojfaktorovou autentifikáciou
 - logovanie systémových udalostí vrátane identifikátora osoby
 - krížová kontrola zmien v konfigurácii / kalibrácii
 - štatistické spracovanie meraných dát s vyhodnotením nezmyslov
 - vylúčenie možnosti úmyselného vytvorenia chybových stavov
 - bezpečnostný **audit a konzultácia** vášho projektu s odborníkmi na kybernetickú bezpečnosť

Ďakujeme za pozornosť.

ENVIRONEXT ►►