4. BEZPEČNOSTNÍ AUDIT VE VYBRANÉ ORGANIZACI

Organizace, kterou jsem si pro potřebu diplomové práce vybral, je organizací cestovního ruchu působící na daném trhu již od roku 1928. Jedná se o hotel Parkhotel Golf Mariánské Lázně, a. s. v kategorii **** s ubytovací kapacitou 52 lůžek. Hotel v současné době zaměstnává 40 zaměstnanců. V souvislosti s rozvojem informačních technologií využívá organizace od roku 1996 vlastní hotelový informační systém, pomocí kterého shromažďuje informace o svých bývalých i současných hostech. Tyto informace pomáhají např. k vytvoření různých druhů statistik a analýz o sezónní a roční obsazenosti hotelu a o národnostní struktuře ubytovaných hostů. Na základě výsledků těchto analýz se organizace rozhoduje o přístupu na další konkurenční trhy, o rozšíření doplňkových služeb hotelu, či o změně cenové politiky. V roce 1997 se hotel stal nestátním zdravotním zařízením. Od toho se odvíjí rozšíření seznamu běžně zpracovávaných citlivých údajů, se kterými organizace cestovního ruchu zachází, o zdravotní stav hostů.

Parkhotel Golf Mariánské Lázně, a. s. zpracovává o svých hostech následující údaje:

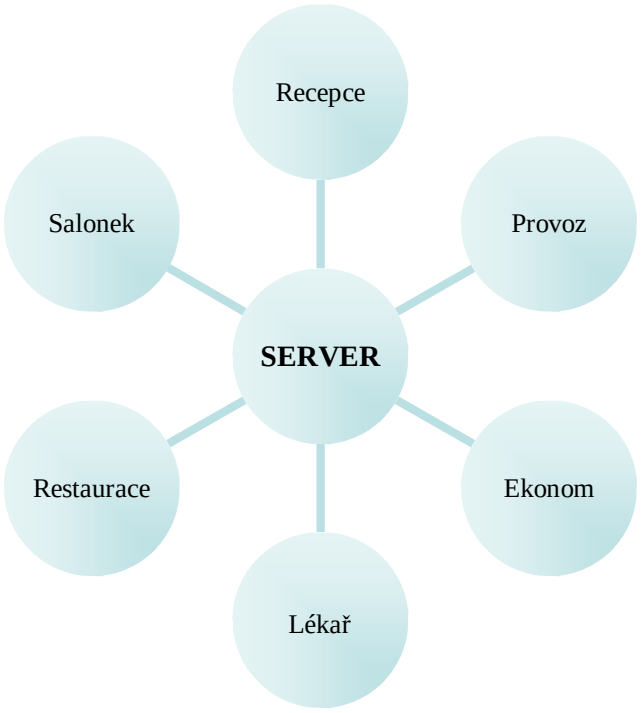
- jméno a přímení,
- bydliště,
- datum narození,
- číslo pasu nebo občanského průkazu (průkazu totožnosti),
- národnost,
- zdravotní stav.

Všechny citlivé údaje (mimo zdravotního stavu hostů) jsou ukládány na server, ke kterému jsou připojeny následující pracoviště:

- recepce,
- provozní oddělení,
- ekonomické oddělení,
- lékař,
- restaurace,
- salonek (počítač pro připojení k Internetu pro hotelové hosty).

Přestože je k serveru připojeno těchto šest oddělení, nahlížet a pracovat s osobními údaji mohou pouze recepce, provozní oddělení, ekonomické oddělení a lékař. Z toho důvodu se v této diplomové práci zaměřím pouze na ty oddělení, které mají k citlivým údajům přístup.

Diagram 1: Připojení jednotlivých oddělení hotelu k serveru



Bezpečnost systému

Fyzická bezpečnost

Fyzickou bezpečnost, jakožto zabezpečení budov, ve kterých je informační systém umístěn, a opatření proti neoprávněnému vniknutí osob, lze sledovat podle pracovišť, na kterých se lze s citlivými údaji v organizaci setkat.

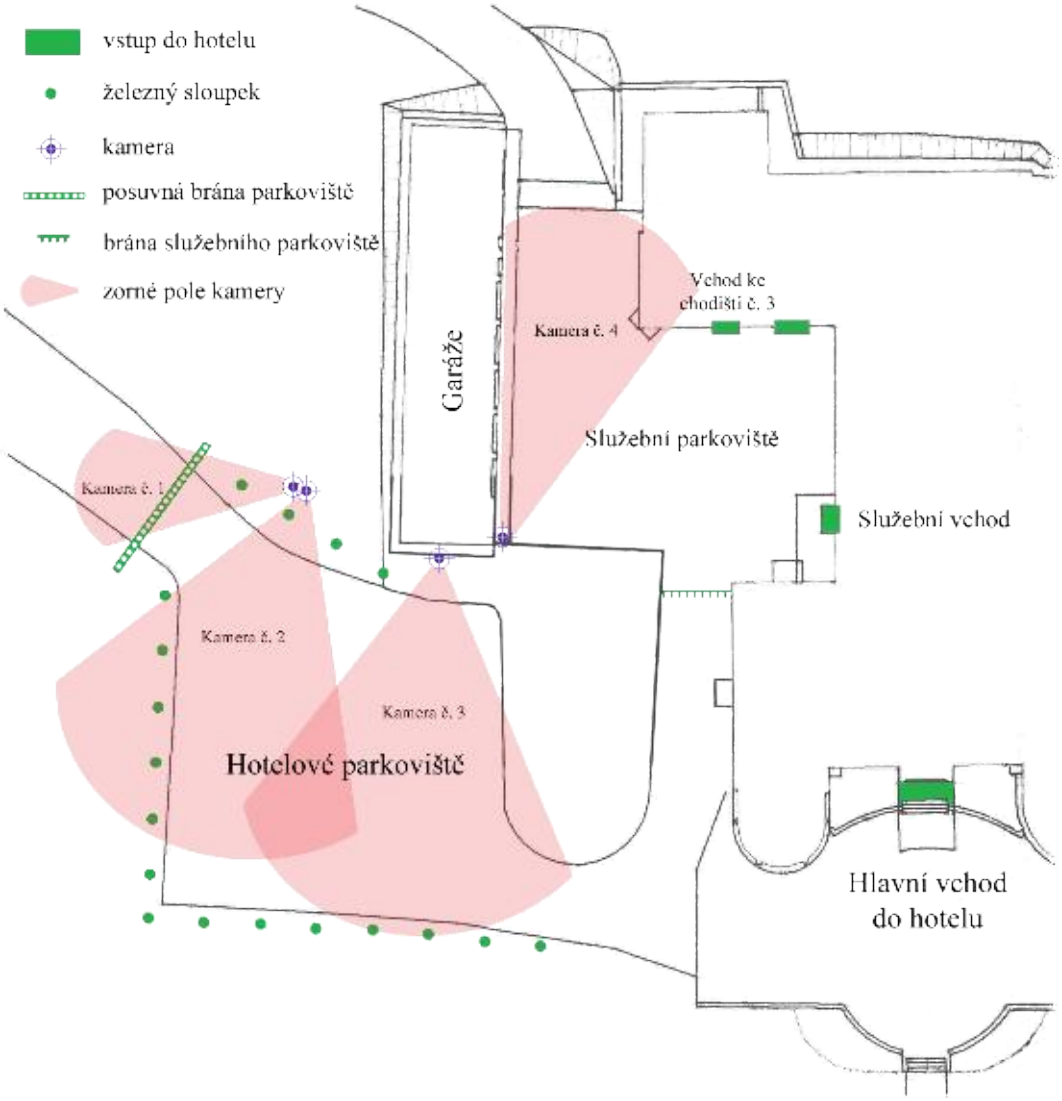
Celkový přístup na pozemek hotelu

Hotel Parkhotel Golf Mariánské Lázně, a. s. se nachází na vlastním pozemku o rozloze 4,7 hektaru. Pozemek je na severní a západní straně ohraničen masivním železným plotem, z východní strany ho uzavírá živý plot a na jižní straně pozemek navazuje na zemědělskou

půdu. Vjezd i vchod na pozemek hotelu jsou na severní straně a ani jeden z nich není opatřen vraty nebo závorou.

Na pozemku hotelu jsou vybudovány dvě parkoviště (hotelové a služební) a garáž se 4 místy k parkování.

Obrázek 1: Pozemek hotelu – parkoviště



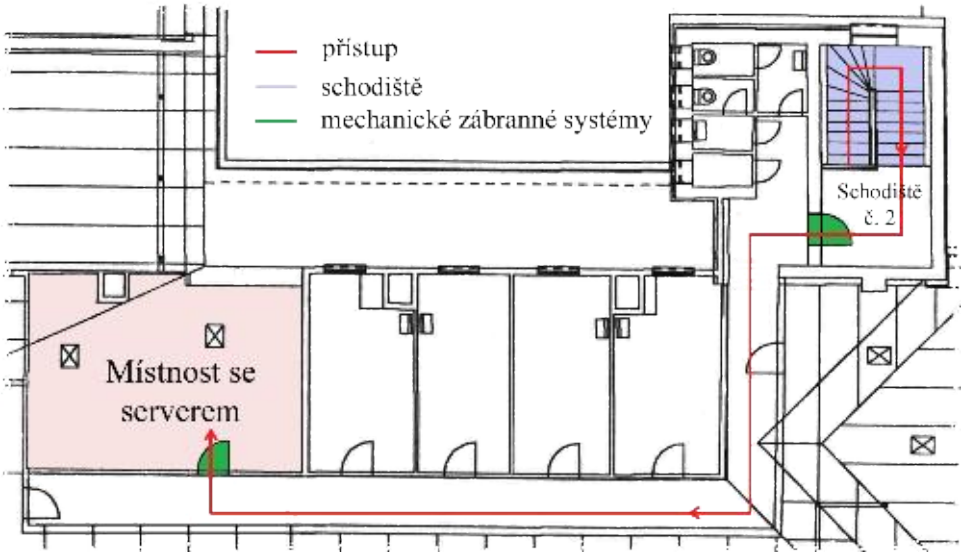
Hotelové parkoviště disponuje kapacitou 18 parkovacích míst a lemuje ho plot zhotovený ze železných sloupků vzdálených od sebe 1,5 metru. Uzavření parkoviště zajišťuje železná posuvná brána s elektrickým pohonem, která je dálkově ovládána z recepce hotelu. Služební parkoviště se nachází na dvoře hotelu, činí 8 parkovacích míst a obklopuje ho garáž a samotná budova hotelu.

Bezpečnost parkovišť a garáží zajišťují 4 bezpečnostní kamery, které pokrývají téměř celou plochu parkovišť. Veškeré dění na těchto prostranstvích se promítá na monitor umístěný na recepci hotelu. Kamera č. 1 snímá příjezdovou cestu a posuvnou bránu hotelového parkoviště. Kamery č. 2 a č. 3 monitorují celou plochu hotelového parkoviště. Jsou umístěny tak, aby se jejich zorná pole překrývala a tím pádem nevznikal tzv. mrtvý bod. Poslední kamerou, která přispívá k fyzické bezpečnosti, je kamera č. 4 kontrolující příjezdovou cestu na služební parkoviště a prostranství před garážemi.

Místnost se serverem

V nedávné době došlo k modernizaci místnosti, ve které se server nachází. Ten je umístěn ve 3. nadzemním patře, které je z 2. nadzemního patra přístupné pouze jedním schodištěm (schodiště č. 2). Zdi místnost jsou zhotoveny z nehořlavého sádrokartonu s protipožární úpravou.

Obrázek 2: 3. nadzemní patro – místnost se serverem



V místnosti se nachází dvě skříně z nehořlavého materiálu, v nichž jsou umístěny rozvody telefonů a Internetu do jednotlivých pokojů, rozvod televizního signálu po hotelu. Dále se zde v místnosti nachází již zmiňovaný server. Server je napojen na vlastní zdroj elektrického napětí, jehož hlavní vypínač se nachází v uzamčené místnosti v přízemí hotelu. K této místnosti (místnost je bez oken) mají přístup pouze zaměstnanci provozního oddělení, recepce a údržby prostřednictvím jednotného klíče. Jak server, tak rozvody telefonů a Internetu do pokojů jsou vybaveny záložním zdrojem elektrické energie (UPS).

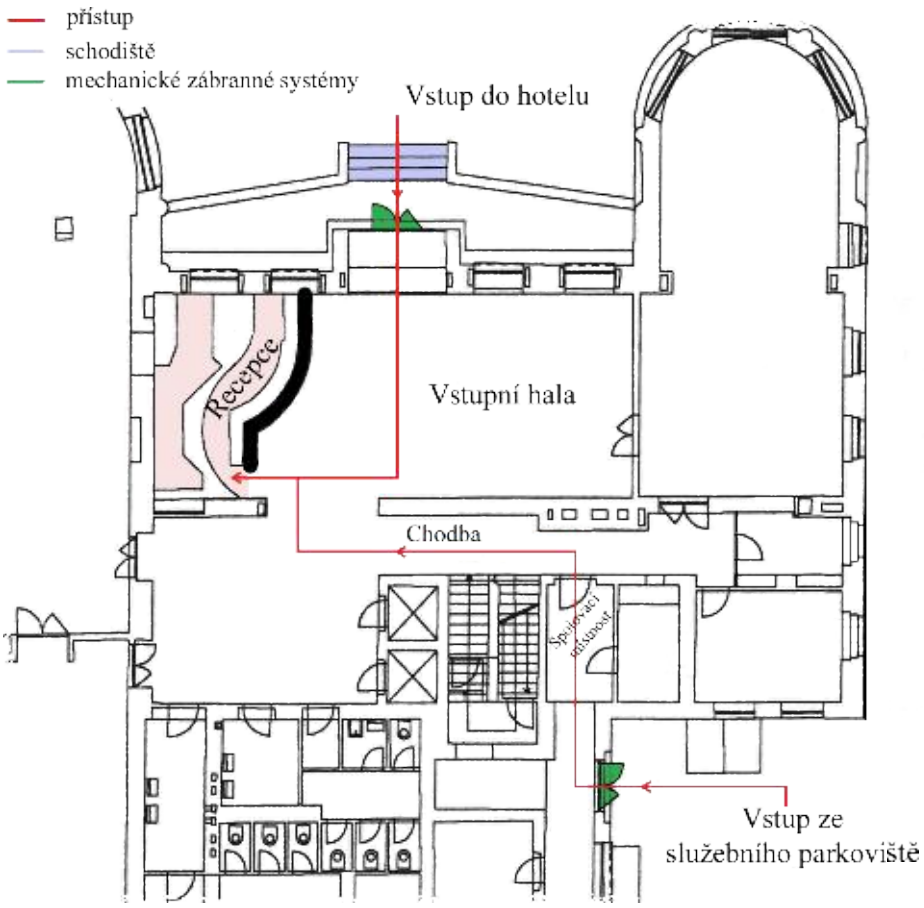
Na přístupové cestě k místnosti se serverem jsou jedinou „překážkou“ dvě mechanické zábrany – dveře. Ty první, skleněné, jsou v těsné blízkosti schodiště. Nejsou opatřeny koulí, jsou zavřené, avšak nejsou zamčené. Druhé dveře slouží jako vchod do samotné místnosti se severem, jsou dřevěné a zamčené.

Od dveří do místnosti se severem existují 4 kusy klíčů, ty mají pouze zaměstnanci provozního oddělení (3 ks) a správce sítě (1 ks).

Recepce

Recepce hotelu je místem, kde se přichází do styku s citlivými údaji každý den. Recepce se nachází v přízemí hotelu – v hotelové hale. Tento prostor nelze technicky zabezpečit uzamčením a proto je zajištěno jen individuální uzamykání skříněk a zásuvek, jedinou zábranou je dřevěný recepční pult. K recepci se lze dostat dvěma možnými přístupovými cestami.

Obrázek 3: Přízemí – recepce



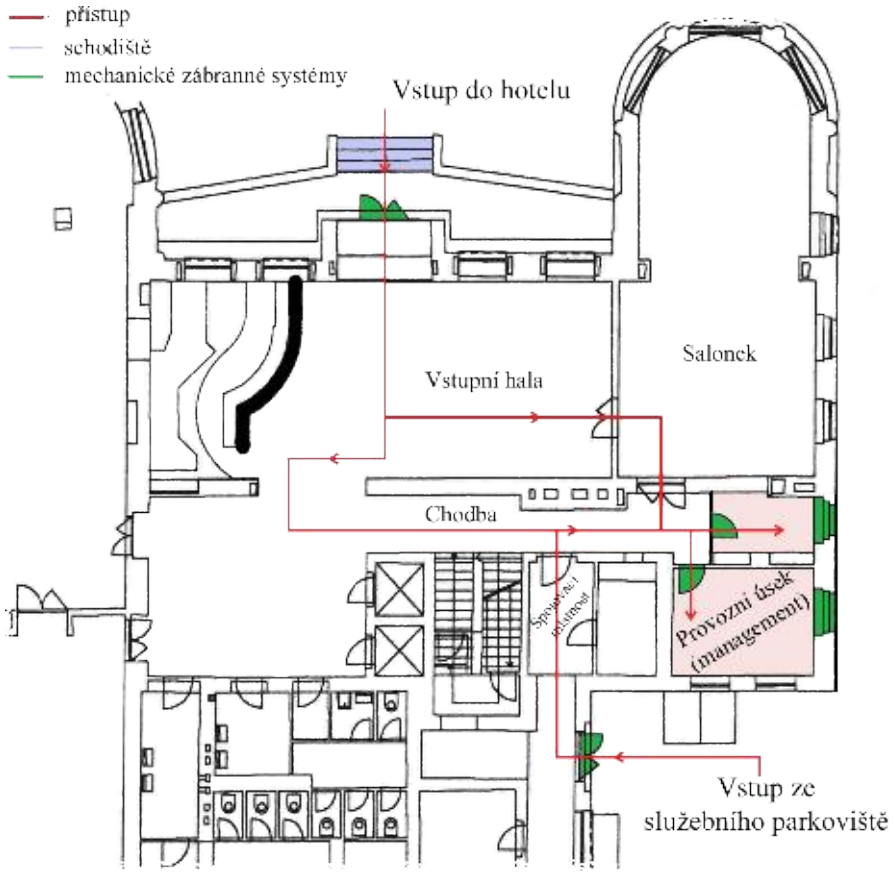
První přístupová cesta vede hlavním vchodem do hotelu, který tvoří dvojité skleněné dveře s čidlem pohybu. Druhou možností přístupu k recepci, je využít služebního vchodu ze služebního parkoviště. Prochází se spojovací místností, poté chodbou až do vstupní haly, kde se recepce nachází. Jediným zábranným systémem jsou zde dveře služebního vchodu, které jsou pro potřeby zaměstnanců hotelu neustále otevřeny. Dveře jsou železné se skleněnými okýnky, přes které jsou namontovány železné mříže.

Dveře se zamykají pouze ve večerních hodinách, po odchodu veškerého personálu. Klíč od těchto dveří je po dobu jejich uzamčení ponechávám v zámku z vnitřní strany, aby nebylo možné se do objektu dostat jiným klíčem. Tento klíč zabezpečuje službu konající recepční, je předáván po ukončení služby.

Provozní oddělení – vedení hotelu

Provozní oddělení se, stejně jako recepce, nachází v přízemí hotelu. Toto oddělení je rozděleno do dvou sousedících kanceláří, jedna pro ředitele hotelu, druhá pro vedoucího provozu.

Obrázek 4: Přízemí – provozní oddělení



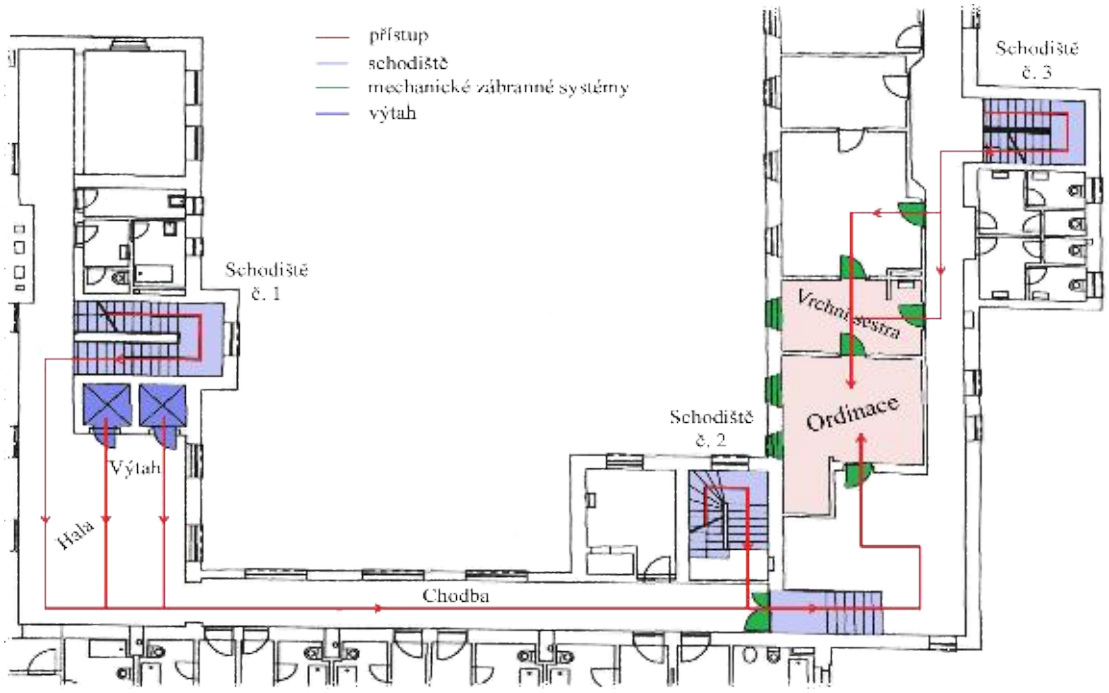
Okna kanceláří jsou opatřena mřížemi, pro zamezení nežádoucího vstupu a možnosti krádeže. Dveře jsou dřevěné a uzamykatelné, přesto často dochází, v případě krátkodobého odchodu některého ze zaměstnanců provozního oddělení, pouze k jejich přivření či uzavření, nikoliv k uzamčení. Tím se samozřejmě zvyšuje nebezpečí ztráty a odcizení důležitých údajů a dokumentů.

Do prostor provozního oddělení je možný přístup opět dvěma cestami. První přístupová cesta vede hlavním vchodem do hotelu, jak již bylo zmíněno u přístupové cesty k recepci. Prochází se vstupní halou kolem recepce, přes chodbu nebo salonek, až ke kancelářím provozního oddělení. Druhá cesta vede služebním vchodem ze služebního parkoviště. Opět téměř jedinou překážkou na této cestě jsou již popisované železné dveře.

Lékař a ordinace

Prostory vymezené pro ordinaci (místnost lékaře) a místnost vrchní sestry se nacházejí v prvním patře hotelu. V ordinaci je umístěn lékařův stolní počítač, kam jsou ukládány záznamy o zdravotním stavu hosta. V této místnosti se dále nachází skříně s formuláři a tiskopisy týkající se dalších podrobných zpráv a indikací o zdravotním stavu hostů, kteří již svůj léčebný pobyt v hotelu ukončili. V místnosti vrchní sestry jsou umístěny skříně s chorobopisy hostů, kteří jsou v hotelu ubytováni.

Obrázek 5: 1. nadzemní patro – lékař a ordinace

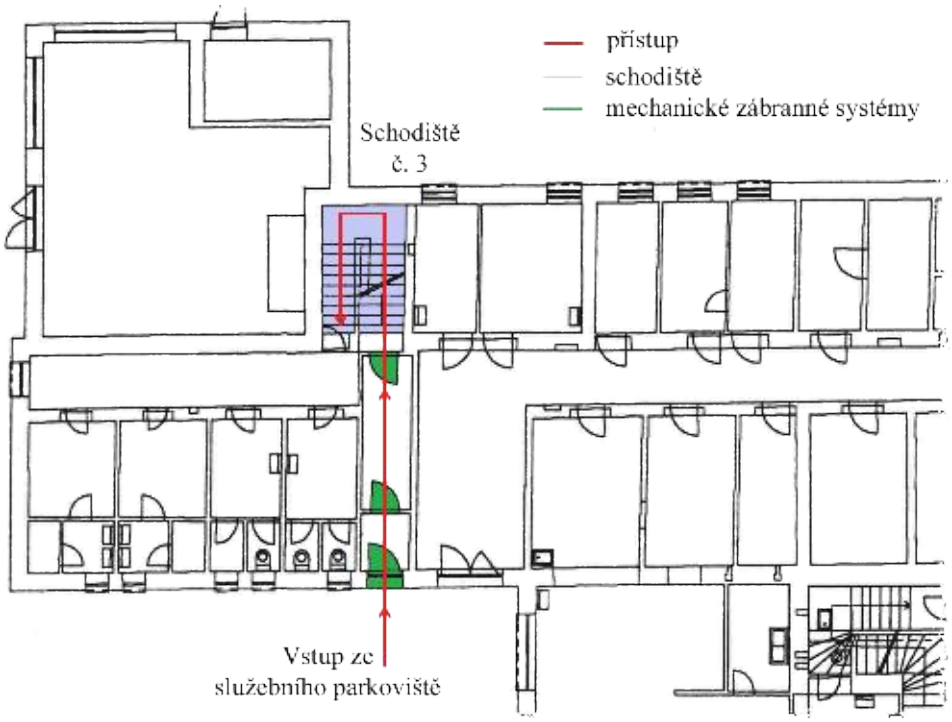


Do těchto prostor existují tři možné cesty přístupu. Všechny cesty vedou po schodech, nebo s využitím výtahů z přízemí hotelu. První cesta vede po schodišti č. 1 (popř. s využitím výtahu) přes malou halu a dlouhou chodbu k první překážce, kterou jsou skleněné dveře. Zde se také napojuje druhá přístupová cesta vedoucí po schodišti č. 2. Tuto druhou cestu bych z hlediska přístupu z přízemí hodnotil jako bezpečnou, jelikož se jedná o služební schodiště a pravděpodobnost povšimnutí si neoprávněného vstupu je zde veliká.

Skleněné dveře jsou tvořeny nerozbitným a ohnivzdorným sklem, během dne jsou otevřené. Tyto dveře se po dobu nepřítomnosti zdravotnického personálu zavírají, avšak nezamykají, a to z toho důvodu, že tyto dveře slouží jako požární únikový východ.

Poslední možnou přístupovou cestou do prostor ordinace a místnosti vrchní sestry je využití východního schodiště hotelu (schodiště č. 3) ze služebního parkoviště. Z této přístupové strany se v prvním patře neobjevují žádné zábranné systémy. Přístup je omezen pouze na úrovni přízemí, kde se nacházejí troje dveře. První jsou dřevěné protipožární dveře, které jsou přes den odemčeny, na noc se zamykají. Druhé dveře zůstávají neustále otevřené. Poslední (třetí) dveře jsou tvořeny nerozbitným a ohnivzdorným sklem, na vnější straně dveří je umístěna koule a dveře jsou stále uzamčeny.

Obrázek 6: Přízemí - schodiště č. 3



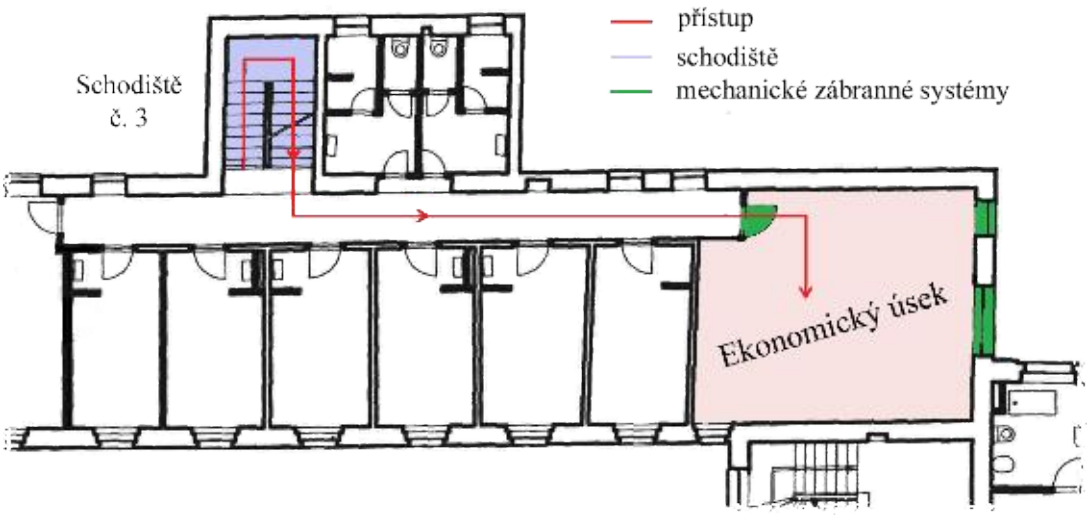
Neoprávněnému vstupu do samotných místností brání silné dřevěné uzamykatelné dveře. Klíče od těchto místností mají pouze lékař, vrchní sestra a zaměstnanci provozního oddělení. Jeden náhradní (rezervní) klíč je pro potřeby havarijního stavu nebo požáru uložen v zapečetěné obálce na recepci hotelu. Okna ordinace a místnosti vrchní sestry nejsou opatřena mřížemi, nacházejí se ve výšce 4 m od země, což se jeví jako zabezpečené. Pouze malou nevýhodou se zde shledávám okapovou stříšku, která je ve výšce kolem 2,5 metru, což by mohlo být pomocným přístupovým bodem, pokud se narušitel do zmíněných prostor bude chtít dostat oknem.

Ekonomické oddělení

Ekonomické oddělení se nachází ve druhém nadzemním patře zadního traktu hotelu. Jedinou přístupovou cestou z prvního patra je po schodišti č. 3, na kterém se ve druhém patře nenachází žádná mechanická přístupová zábrana. Jak již bylo zmíněno u popisu fyzického zabezpečení ordinace a místnosti vrchní sestry, přístup je omezen na úrovni přízemí, kde se nacházejí dřevěné protipožární a skleněné ohnivzdorné dveře.

Dveře místnosti jsou ze dřeva, uzamykatelné, a klíče jsou vyhotoveny ve 4 kusech. Dva kusy vlastní zaměstnanci ekonomického oddělení, zbylé dva zaměstnanci provozního oddělení. Okna jsou malá, nezamřížovaná, a nacházejí se ve výšce 5 m nad zemí, což slouží jako dostatečné zabezpečení místnosti.

Obrázek 7: 2. nadzemní patro – ekonomické oddělení

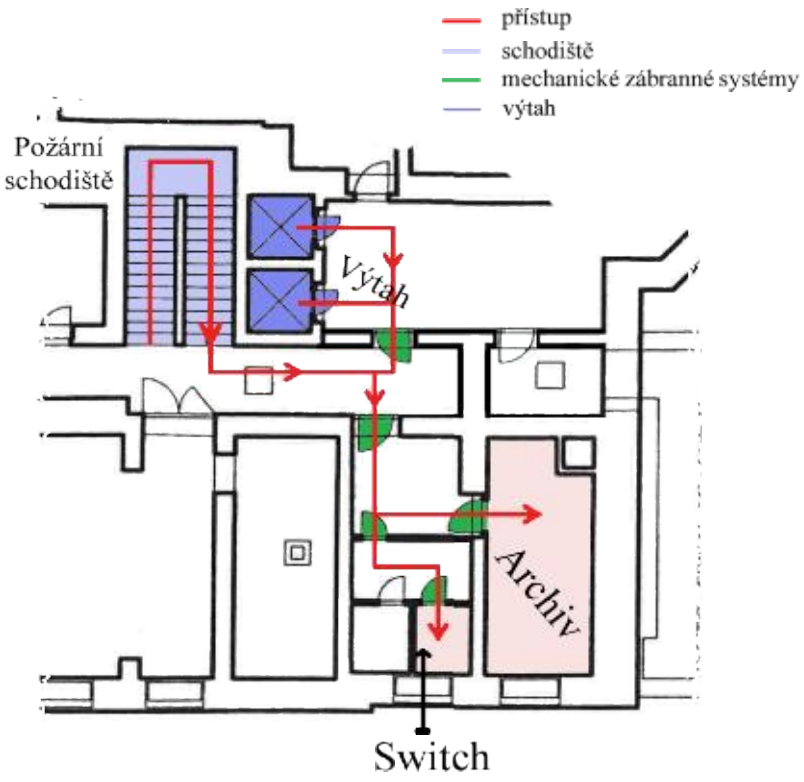


Archiv uložených záznamů

Poslední důležitou místností, kde se lze s citlivými údaji setkat, je archiv. Tato místnost se nachází v prvním podzemním patře, je bez oken a v hloubce tří metrů pod povrchem země. Prakticky jedinou možnou cestou, jak tohoto patra dosáhnout, pomineme-li přístup po požárním schodišti, které je pro laika jen těžko objevitelné, je použití výtahu. Na přístupové cestě od výtahu k archivu se musí překonat 4 zábranné systémy – dveře, z nichž pouze dvoje jsou uzamčené. Tím se samozřejmě zvyšuje riziko neoprávněného vniknutí do místností.

První dveře zůstávají neustále otevřené pro potřeby personálu, který je využívá pro přístup do skladovacích prostor hotelu. Druhé dveře ze silného dřeva jsou uzamčené, navíc nejsou ani označené, tudíž nelákají pozornost. Dveře do samotného archivu zůstávají otevřené, důvodem je cirkulace vzduchu ze vzduchotechniky, která udržuje teplotu vhodnou pro archivaci tiskopisů (převážně o hospodaření organizace) a datových zdrojů. Posledními uzavřenými dveřmi jsou ty, které vedou do místnosti, kde se nachází aktivní prvek hotelové sítě – switch a ISDN LAN modem pro připojení hotelové počítačové sítě do Internetu.

Obrázek 8: 1. podzemní patro – archiv



Klíče od těchto místností jsou umístěny v trezoru provozního oddělení a na oddělení ekonomickém.

Personální bezpečnost

Zaměstnanec představuje pro organizaci potenciální hrozbu, proto je na jeho výběr, přijímání a následné vzdělání kladen velký důraz, obzvláště v oblasti citlivých údajů.

Výběr nových zaměstnanců

Přijímací řízení, výběr a posuzování požadované způsobilosti zaměstnanců probíhá za úzké spolupráce provozního a ekonomického oddělení a příslušných vedoucích zaměstnanců. Při výběru zaměstnanců, kteří budou vykonávat svou činnost v oblasti, která v sobě zahrnuje i zpracování a zacházení s citlivými údaji, pomáhá hotelu personální agentura. Nástupy nových zaměstnanců zajišťuje v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a na základě výsledků výběrových rozhovorů provozní oddělení.

Základní příprava a zaškolení nových zaměstnanců

Nástupní školení zaměstnance provádí provozní oddělení. Jedná se o ústní seznámení nového zaměstnance s právy a povinnostmi vyplývajícími z pracovního poměru, se zdroji informací ve firmě, s používanými systémy, atd.

Recepce

Nově přijatý zaměstnanec je seznámen se svou pracovní náplní, s bezpečnostními předpisy a směrnicemi organizace. Jelikož se jedná o pracoviště, kde se zaměstnanec setkává s citlivými údaji každý den, není nově přijatému zaměstnanci heslo do systému a do ostatních aplikací sděleno ihned, nýbrž až v průběhu zkušební doby. Tím se organizace chrání před zneužitím či odcizením citlivých osobních údajů.

Je-li zaměstnanec shledán způsobilým vykonávat tuto činnost, je mu vedením hotelu vytvořen uživatelský účet (uživatelské jméno a heslo). Heslo je možné si po domluvě s vedením hotelu vybrat samostatně. Toto heslo je poté zapsáno do systému a do kontrolního seznamu hesel, který je uložen v trezoru v kanceláři provozního oddělení. Dále jsou zaměstnanci recepce vystavena další dvě hesla pro přístup do recepčního systému a do programu na správu karet pro vstup do hotelových pokojů.

Ihned po vytvoření uživatelského účtu je možné se přihlásit do informačního systému hotelu.

Ve vytvořeném uživatelském účtu nemá zaměstnanec oprávnění upravovat si vlastní přístupová práva ke zdrojům informačního systému. Hesla jsou platná po dobu jednoho roku. Vždy jeden den před vypršením platnosti se hesla obnovují (popř. mění, což není podmínkou). Zaměstnancům dále není dovoleno upravovat konfiguraci ať už jednotlivých částí, nebo celého informačního systému (to je povoleno pouze správci sítě, a to po dohodě a se souhlasem provozního oddělení). Zaměstnanci si nemohou instalovat žádné vlastní programy.

Provozní oddělení

Při přijímání nového zaměstnance na volné místo provozního oddělení je zaměstnanec poučen o svých pravomocech a seznámen s náplní vykonávané práce. Zaměstnanci není vytvořen žádný uživatelský účet, pouze je mu, proti podpisu, sděleno přihlašovací jméno a heslo k počítači na tomto oddělení.

Vedoucí provozu má na rozdíl od ředitele hotelu omezené možnosti ve využívání všech dostupných funkcí jednotlivých programů. Nemá oprávnění nahlížet do výkazů ekonomického oddělení, může pouze sledovat objem denních tržeb, stav obsazenosti hotelu a může nahlížet do restauračního programu, a tím kontrolovat vyúčtování prodeje zboží a služeb na středisku restaurace. Další funkcí, kterou má vedoucí provozu na starosti, je kontrola stavu zásob skladového hospodářství.

Ekonomické oddělení

Nový zaměstnanec ekonomického oddělení je opět seznámen se svou pracovní náplní, navíc je seznámen se směrnicemi nejen vlastní organizace, ale i se směrnicemi ostatních subjektů, jakými jsou peněžní úřady, finanční úřady, státní správa, atd. Novému zaměstnanci je rovněž sděleno přihlašovací jméno a heslo k počítači na ekonomickém oddělení. Tím automaticky získává oprávnění využívat různé ekonomické programy a analytické nástroje sloužící k hodnocení finančního stavu hotelu.

Stejně tak jako provozní oddělení, nemůže nahlížet do výkazů ekonomického oddělení, ekonomické oddělení nemůže nahlížet do výkazů a přehledů oddělení provozního. Mezi hlavní náplň práce, kterou zaměstnanec na ekonomickém oddělení provádí patří

sestavování přehledů hospodaření – účetní rozvahy, výkazu zisků a ztrát, roční účetní uzávěrky; proplácení fakturací a v neposlední řadě komunikace s bankovními a finančními institucemi.

Lékař a vrchní sestra

Dojde-li k zaškolování nového hotelového lékaře nebo vrchní sestry, je jim sdělena pracovní náplň související s jejich oddělením. Vedení hotelu sdělí novému zaměstnanci přístupové jméno a heslo k počítači na daném oddělení. Přístupovým heslem je zároveň uděleno oprávnění využívat specifické lékařské programy, lékařské dekurzy, přehledy léků a indikací, seznamy provedených vyšetření. Dále jsou seznámeni s používáním všech zdravotnických přístrojů, s umístěním léků a zdravotnického materiálu. Lékař je povinen ukládat zprávy o zdravotním stavu jednotlivých pacientů na pevný disk počítače, nikoliv na server, a tyto údaje měsíčně zálohovat. Zaměstnanec musí používat pouze programové vybavení v majetku hotelu a nesmí do počítače instalovat svůj soukromý nebo nelegální software.

Lékař i vrchní sestra společně využívají jeden počítač.

Zaměstnanci využívající tento počítač nemohou nahlížet do výkazů ekonomického oddělení, ani do výkazů a přehledů provozního oddělení.

Průběžné zvyšování kvalifikace personálu

Parkhotel Golf Mariánské Lázně, a. s. zabezpečuje vzdělávání, školení a rozvoj svých zaměstnanců prostřednictvím provozního oddělení, které má na starosti plán vzdělávání zaměstnanců. Plán vzdělávání vychází z provozních potřeb organizace a to zejména z výsledků ročního hodnocení pracovní výkonnosti.

Ukončení pracovního poměru

Při rozvázání pracovního poměru je odcházející zaměstnanec poučen o svých povinnostech vůči bývalému zaměstnavateli, a po jeho odchodu ze zaměstnání se kladou požadavky na mlčenlivost.

Každému zaměstnanci využívajícímu uživatelský účet je tento účet při ukončení pracovního poměru zrušen.

Externí a dočasní pracovníci

Hotel Parkhotel Golf Mariánské Lázně, a. s. nenajímá žádné externí, ani dočasné pracovníky na pracoviště zpracovávající citlivé údaje.

Datová bezpečnost

Datová bezpečnost je jedním z nejdůležitějších aspektů výstavby a provozu systému, proto se jí věnuje značná pozornost.

Téměř veškerá data, se kterými se na jednotlivých střediscích pracuje, se ukládají na disk serveru. K zamezení ztrátě dat při poškození disku, využívá server dvou zrcadlových disků. Fyzický přístup k serveru má pouze provozní oddělení a správce sítě, který jako jediný může zasahovat do softwarového a hardwarového vybavení serveru.

Funkci systému řízení báze dat (SŘBD) zde naplňuje hned několik programových prostředků, podle toho, na kterém pracovišti se s daty pracuje. Mezi tyto systémy řízení báze dat patří:

- recepční program,
- restaurační program,
- skladové hospodářství,
- zdravotní dokumentace,
- mzdové programy,
- evidence HIM a DHIM.

Jednotlivá oddělení pracují s různými citlivými údaji.

Recepce

Zaměstnanci recepce mají jako jediní v celém hotelu možnost citlivá osobní data ubytovaných hostů nejen číst, ale také editovat. Při příjezdu nového hosta zapíší již dříve zmíněné citlivé údaje do recepčního programu, k těmto údajům je doplněno číslo pokoje. Číslo pokoje se od této doby stává identifikátorem hosta po dobu jeho pobytu v hotelu, a pod tímto číslem je záznam uložen na serveru. Veškeré operace přihlášeného uživatele jsou, pro zpětnou kontrolu, sledovány serverem a zapisovány do souboru na disk serveru (viz kapitola 4.2.6).

K těmto údajům jsou postupně doplňovány další údaje typu:

- platby za různé druhy zboží a poskytnutých služeb,
- platby za připojení k Internetu,
- platby za telefonní hovory,
- platby za provedené lékařské vyšetření,
- platby za léky, atd.

Při odhlášení hosta (vyrovnání účtu) je jeho záznam na serveru přesunut a uložen do složky archiv hostů. Číslo pokoje, jakožto identifikátor hosta, se tímto krokem uvolní pro další rezervovaný pobyt.

Provozní oddělení

Žádný zaměstnanec provozního oddělení, ať už je to vedoucí provozu, nebo samotný ředitel hotelu, nemá oprávnění editovat citlivé údaje, které byly do systému vloženy zaměstnancem recepce. Provozní oddělení může pouze nahlížet do záznamů na serveru pomocí programů SŘBD, konkrétně pomocí recepčního programu, mzdových a evidenčních programů.

Ekonomické oddělení

Práce ekonomického oddělení s citlivými údaji se převážně vztahuje na zpracování údajů o samotné společnosti. Těmito údaji mohou být výsledky hospodaření, rozvahy, výkazy zisků a ztrát, přehled cash flow, evidence HIM a DHIM a mzdová agenda. Všechny tyto údaje může ekonomické oddělení jak číst, tak editovat.

Ekonomické oddělení může také nahlížet do stavu obsazenosti hotelu a přehledu rezervací na následují období, ale jediné údaje, které jsou tomuto oddělení přístupné, jsou číslo pokoje, jméno a příjmení hosta (např.: 106 – Josef Pinkr).

Spolu s provozním oddělením spravuje personální agendu, do které nemá recepční oddělení oprávněný přístup.

Lékař

Práce na zdravotním oddělení spolu s recepčním oddělením patří k nejdůležitějším, co se zpracování citlivých osobních údajů týče. Lékař potřebuje znát údaje o hostech, proto si ze serveru do svého zdravotnického programu načítá základní údaje hostů, kterými jsou:

- jméno a příjmení,
- datum narození,
- bydliště,
- národnost,
- počet minulých pobytů.

Záznam o počtu minulých pobytů slouží lékaři pro informaci zda se zde již host léčil, a pokud ano, pak lékař z archivu, pomocí základních údajů o hostu, načte seznam minulých chorobopisů.

K těmto údajům doplňuje zdravotní stav hostů a dopisuje ho do lékařského formuláře, který následně ukládá na pevný disk svého počítače. Zdravotní oddělení podléhá mimo zákona č. 101/2000 Sb., o ochraně osobních údajů, také lékařskému tajemství. I to je důvodem, proč jsou údaje o zdravotním stavu ukládány na pevný disk počítače a ne na disk serveru.

Technická bezpečnost

Technická bezpečnost se snaží řešit ochranu dat použitím odpovídajícího technického (softwarového i hardwarového) vybavení. Přispívá k tomu kladení velké pozornosti na jeho výběr, zajištění potřebné spolehlivosti a servisní služby.

Hlavní slovo v technické bezpečnosti organizace má správce hotelové sítě. Ten se stará o modernizaci hardwarového vybavení počítačové sítě, a po konzultaci s provozním oddělením i o instalaci nových programů a aktualizaci programů stávajících. Servis veškerého výpočetního vybavení probíhá dle potřeb provozního oddělení nebo systému samotného.

Mimo zdravotnické oddělení jsou na všech ostatních odděleních k počítačům připojeny záložní zdroje elektrické energie (UPS), jmenovitě recepce, provozní úsek, ekonomický úsek. Jak již bylo zmíněno, na jeden záložní zdroj je také napojen server.

Zálohování dat

Zálohování dat probíhá na všech odděleních. Nejčastějším médiem pro zálohu dat je v současné době CD-R, ale lze se zde setkat i s disketami.

Recepční oddělení zálohuje veškerou svou činnost na disk serveru, a to až několikrát denně, podle počtu vykonaných operací s daty. Na recepci není dostupná žádná zálohovací jednotka, aby vedení hotelu zamezilo krádežím a pokusu o zneužití citlivých osobních údajů hostů, které by si zaměstnanci mohli na daném médiu nahrát a odnést z organizace pryč. Dřívější záznamy o ubytovaných hostech, které jsou uloženy nejen na datových médiích, ale i v tiskové podobě jsou uloženy v archivu Parkhotelu Golf Mariánské Lázně, a. s. I server zálohuje svá data, aby nedošlo k jejich ztrátě a využívá k tomu systému dvou zrcadlových disků.

Provozní oddělení zálohuje svá data jednou měsíčně na média CD-R a v poslední době, při nárůstu datových objemů, začíná využívat i DVD médií. Média s citlivými údaji hostů i samotného hotelu jsou rozděleny podle stáří, starší údaje jsou umístěny do archivu hotelu, aktuálnější údaje jsou ponechány v trezorech, které jsou zabudovány v obou sousedících místnostech provozního oddělení.

U lékaře nebyl na zálohování kladen velký důraz. Až v nedávné době se začaly zálohovat údaje o zdravotním stavu hostů a seznam jejich chorobopisů na média typu CD-R, která jsou z důvodu ochrany osobních údajů a lékařského tajemství archivována na pracovišti zdravotnického oddělení.

Posledním oddělením, které si zálohuje svou činnost a dostává se do styku s citlivými údaji samotné organizace, je ekonomické oddělení. To zálohuje svou činnost vždy na konci dne, využívá k tomu disketových médií a tyto média následně ukládá do skříňového trezoru, který se nachází rovněž na tomto oddělení.

Režimová bezpečnost

Tato bezpečnost je tvořena administrativními opatřeními, nařízeními a systémy kontrol, které zajišťují bezpečnost systému a tím přispívají k respektování právních norem a zákonů. Režimová bezpečnost definuje způsoby, postupy a procedury, které je nutno dodržovat pro zajištění bezpečnosti daného systému. V organizaci jsou to především vnitřní směrnice a pokyny hotelu, etický kodex hotelu, zaměstnanci jsou navíc povinni se seznámit se zásadami bezpečnosti práce na svém pracovišti a dodržovat je.

Dne 15. října 2004 byl Parkhotelu Golf Mariánské Lázně, a. s. udělen společností Mag Consulting, s.r.o. (certifikační orgán pro certifikaci systémů jakosti) CERTIFIKÁT ISO 9001:2001. Tímto je potvrzeno, že hotel má v procesech poskytování lázeňských služeb v oboru fyziatrie, balneologie a léčebné rehabilitace včetně ubytování a stravování zaveden a udržován systém managementu jakosti, který je ve shodě s požadavky normy ČSN EN ISO 9001:2001. V tomto certifikátu se dále mimo jiné v rámci norem ČSN EN ISO 9001:20001 upravují:

- pravidla pro provozování výpočetní techniky a programového vybavení,
- archivní řád,
- spisový řád,
- provozní řád rekondičního a rehabilitačního oddělení, atd.

Kontrola dodržování systému jakosti podle certifikátu ISO 9001:2000 probíhá v Parkhotelu Golf Mariánské Lázně, a. s. dvakrát do roka a zahrnuje v sobě právě i zmíněné dodržování pravidel pro provozování výpočetní techniky a programového vybavení, které úzce souvisí se zacházením s citlivými údaji.

Pravidla pro provozování výpočetní techniky a programového vybavení

Počítačovou síť Parkhotelu Golf Mariánské Lázně, a. s. a externí síť lze používat pouze v souvislosti s plněním pracovních úkolů a ve prospěch organizace. Je zakázáno používat počítačovou síť, počítače, programy, data organizace a přístup na Internet a elektronickou poštu pro soukromé účely, nebo umožnit jejich užívání jiným neoprávněným osobám. Úmyslný a neoprávněný zásah do hardwaru nebo softwaru je považován za hrubé porušení pracovní kázně, a může vést až k rozvázání pracovního poměru se zaměstnancem.

Za neoprávněný zásah se považuje mj. vstup do programu chráněného heslem bez platného oprávnění (např. pod heslem jiné, oprávněné osoby), instalace neschváleného (nelegálního) programu do počítače a změna nebo vymazání dat.

Správce sítě (pracovník externí smluvní servisní firmy ve spolupráci s provozním oddělením) je povinen zaznamenat jakýkoliv neoprávněný vstup do sítě včetně dat a rozsahu. Toto zjištění je nutné zdokumentovat a neprodleně nahlásit provoznímu oddělení hotelu.

Přístupová práva do hotelové sítě

Zaměstnanec, který má přístupové právo do systému, programu nebo k datům umístěných v počítačové síti hotelu pod heslem, musí o heslu zachovávat mlčenlivost, nesmí jej sdělovat dalším pracovníkům a je povinen se přihlašovat pouze pod tímto heslem. Je výslovně zakázáno sdělovat přístupová hesla spolupracovníkům nebo příbuzným.

Přístupová práva do Internetu a elektronické pošty (e-mail)

Přístupová práva jednotlivých zaměstnanců do Internetu zřizuje správce počítačové sítě a provozní oddělení na základě písemného požadavku příslušného vedoucího úseku.

Internet a e-mail lze používat pro komunikaci a zjišťování informací pouze v souvislosti s plněním pracovních úkolů a ve prospěch organizace. Je zakázáno užívat Internet a e-mail pro soukromé účely či umožnit užívání neoprávněným osobám. Porušení tohoto ustanovení je považováno za hrubé porušení pracovní kázně.

Veškeré dokumenty zasílané a přijímané elektronickou poštou je třeba kontrolovat antivirovými programy. Zaměstnanci nejsou oprávněni prostřednictvím elektronické pošty, internetových prohlížečů apod. kopírovat jakékoliv programové vybavení z externích sítí.

Zajištění bezpečnosti sítě

Při používání disket, CD-R, CD-RW a dalších médií je třeba důsledně provádět antivirové kontroly přinesených souborů, nebo souborů doručených poštou. Čtení a kontrolu jiných neběžných druhů médií včetně antivirových kontrol zajistí pracovník provozního oddělení na vyžádání.

Programové vybavení

Instalaci veškerého programového vybavení je oprávněn provádět pouze správce počítačové sítě. Ostatní pracovníci hotelu nejsou oprávněni testovat ani provozovat jakékoliv programy externího původu bez ověření a souhlasu provozního oddělení. Zaměstnanci dále nesmí provádět nelegální kopírování a šíření programového vybavení, jehož licence je ve vlastnictví organizace. Porušení tohoto ustanovení je považováno za hrubé porušení pracovní kázně.

Antivirové programy

Antivirové programy jsou instalovány a udržovány správcem počítačové sítě a provozním oddělením. Uživatelé počítačů nejsou oprávněni z jakýchkoliv důvodů zasahovat do jejich běhu a funkčnosti. Zaměstnanci jsou povinni neprodleně nahlásit jakékoliv příznaky výskytu počítačových virů telefonicky (je zakázáno používat elektronickou poštu) pracovníkovi provozního oddělení.

Zálohování dat

Zaměstnanci jsou povinni důležité soubory, které využívají při své práci, kromě uložení na lokální medium, také zálohovat na síťový disk (obvykle označovány jako F,Y,Z:) do adresáře označeného jejich jménem (//:XY/JMÉNO zaměstnance). Kapacita síťového adresáře je shora omezena. Při nedostatku prostoru pro zálohování souborů je zaměstnanec povinen požádat vedoucího pracoviště o zajištění dalšího prostoru pro zálohování souborů.

Pravidelné zálohování souborů je povinností každého uživatele počítače. Volba alternativního média a způsob zálohování musí být konzultován s pracovníkem provozního oddělení.

Archivní řád

Písemnosti a záznamy na technických nosičích dat se ukládají na pracovišti, kde byly zpracovány nebo kde vznikly, popřípadě v archivu hotelu. Písemnosti se v útvaru ukládají tak dlouho, dokud je jich třeba k běžné práci. O způsobu uložení rozhoduje vždy vedoucí úseku. Odděleně od ostatních písemností se ukládají účetní písemnosti a záznamy.

Před uložením do archivu musí být písemnosti uspořádány a řádně zabezpečeny proti poškození. O předávaných písemnostech se pořídí soupis podle jednotlivých svazků.

Soupis písemností v archivu musí obsahovat:

- pořadové číslo příslušného svazku (spisu, nosiče dat),
- souhrn písemností a záznamů (oddělení, obsah, množství),
- časový rozsah spisu v letech,
- skartační znak (A, S, V),
- lhůtu podle skartačního řádu.

Při uložení do archivu se používají tyto skartační znaky:

- A – archiv písemností, které jsou určeny k trvalému uložení do příslušného archivu,
- S – skartace písemností, které jsou po uplynutí lhůty určeny ke zničení,
- V – výběr písemností, o nichž nelze v současnosti rozhodnout, a až po uplynutí podle skartačního řádu se rozhodne o skartaci nebo o archivaci.

Skartační lhůtou se rozumí doba, po kterou se písemnost označená znakem (A, S, V) uschová v archivu společnosti. Skartační lhůta se počítá od 1. ledna následujícího roku po vyřízení písemnosti.

O utajovaných skutečnostech rozhodne představenstvo akciové společnosti, případně ředitel hotelu s ohledem na § 17 až § 20 obchodního zákoníku[4] [32], jako o obchodním tajemství, které je časově neomezené. Za obchodní tajemství lze považovat např. i seznam prodávajících, kupujících, obchodní plány, vedení a obsah obchodních knih, kalkulace, dokumentace, vnitřní předpisy, ekonomické a investiční plány a zápisy z představenstva.

Skartaci zajišťuje jednou ročně ekonomické oddělení za účasti příslušného oddělení. Skartační návrh podepisuje před skartací výhradně ředitel hotelu.

Likvidaci lze provést až po rozhodnutí o dalším nakládání se znakem A a po vydání souhlasu ředitele hotelu ke znakům S a V. Do této doby je povinnost zajistit písemnosti proti ztrátě, zničení nebo poškození.

Zabezpečení archivace

Odpovědností za uložení a evidenci účetních dokladů a písemností, správu účetního archivu, uložení a evidenci mzdových dokladů a písemností, uložení a evidenci ostatních dokladů a písemností. je pověřen vedoucí ekonomického úseku. Vybraní zaměstnanci odpovídají za dodržování předpisů a podmínek uložení archiválií.

Při zániku účetní jednotky přecházejí písemnosti na jejich právní zástupce. Pokud neexistuje žádný právní zástupce, mohou účetní jednotky vyřadit účetní písemnosti až po vypořádání jejich majetku a závazků, nestanoví-li právní předpis jinak. Vedoucí zaměstnanci jsou povinni seznámit s tímto řádem zaměstnance a zajistit uvedené postupy.

[4] Zákon č. 367/2000 Sb. a zákon č. 370/2000 Sb.

Spisový řád

Všechny činnosti, které jsou při manipulaci s písemnostmi vykonávány, jsou zahrnuty pod pojmem spisová služba. Spisová služba je souhrnem činností spojených s manipulací písemností směrem od/k externím subjektům. Rozhodující činnosti spisové služby jsou zahrnuty do působnosti úseku provozního a ekonomického oddělení.

Recepce provádí činnosti týkající se převzetí doručených (došlých) písemností, zaevidování doporučených došlých písemností do knihy doručených písemností, opatření došlých písemností presentačním razítkem s datem doručení, a vytřídění písemností pro vedení hotelu (jedná se o písemnosti adresované pro ředitele hotelu, představenstvo akciové společnosti a dozorčí radu akciové společnosti, dále o písemnosti došlé ze zahraničí, od orgánů státní správy, reklamace, urgence a stížnosti).

Odpověď na došlou písemnost nebo písemné informace zajišťuje ředitel hotelu osobně nebo jeho zástupce, popř. osoby pověřené k této činnosti.

Režimová bezpečnost se také zabývá postupem při připojení nového počítače do systému, vytvoření nebo zrušení uživatelského účtu, popř. nastavením přístupových práv do systému. Všechny tyto postupy již byly popsány v předcházejících kapitolách.

Komunikační bezpečnost

Parkhotel Golf Mariánské Lázně, a. s. využívá pro připojení pracovních stanic k lokální síti hvězdicovou síťovou topologii, ve které je server středovým prvkem sítě. Ten rozvádí signál k jednotlivým počítačům prostřednictvím aktivního prvku, kterým je v této síti switch.

Přístup k Internetu zprostředkovává ISDN LAN modem, ten se nachází v prvním podzemním patře hotelu, v místnosti sousedící s archivem. Tento modem je připojen k serveru a ochranu před možnými útoky ze strany Internetu zabezpečuje firewall, který je součástí bezpečnostního systému serveru.

Lokální počítačová síť vznikla především z potřeby sdílet data a údaje nejen o ubytovaných hostech, ale i o ekonomických výkazech a provozních přehledech. Většina programů je nainstalována přímo na jednotlivých pracovních stanicích a plní funkci systémů řízení báze dat, která jsou uložena na serveru. Tyto programy jsou s daty

na serveru úzce propojeny a v případě výpadku serveru, nejen že nelze načítat potřebné údaje z jeho disku, ale ani nelze používat programy, které s těmito daty pracují.

Komunikační bezpečnost je na nejvyšší úrovni řešena pomocí uživatelských účtů, na základě přístupových práv a hesel. Server sleduje jednotlivé činnosti přihlášeného uživatele a jeho kroky zapisuje do souboru na disk serveru. Při zpětném dohledávání je pak snadno zjistitelné, kdo, kdy a jakým způsobem provedl danou operaci, zacházel s danými údaji a informacemi, či se dokonce snažil zasahovat do daného systému.

Organizace při ukládání a zálohování dat (disk serveru, nebo disk osobního počítače) nepoužívá žádné kryptografické ochranné prvky – šifrovací klíče. Jedinými ochrannými prvky, které hotel používá, jsou certifikační klíče pro komunikaci s bankovními institucemi. Tyto klíče vlastní ředitel hotelu a zaměstnanci ekonomického oddělení (každý z nich má svůj vlastní verifikační klíč).

Proces řízení bezpečnosti

Parkhotel Golf Mariánské Lázně, a. s. se problematikou procesního řízení bezpečnosti nezabývá. Základní procesní řízení bezpečnosti je řešeno na základě certifikátu jakosti ISO 9001:2000, který je ve shodě s požadavky normy ČSN EN ISO 9001:2001, a dále pak na základě pravidel pro provozování výpočetní techniky a programového vybavení.

Ochranné systémy

V popisované organizaci se využívají tyto ochranné systémy.

Monitorovací systémy

Elektrické zařízení řízeného vstupu a pohybu

Tento ochranný monitorovací systém není v organizaci nainstalován. Nabízí se zde otázka, zda-li je to vůbec nezbytné. Dalo by se říci, že tuto monitorovací funkci plní zaměstnanci hotelu (jmenovitě: zaměstnanci recepce, obsluhy, provozního oddělení a house keepingu). Ti po dobu 24 hodin dohlížejí na pohyb hostů a osob v budově hotelu i mimo ni.

Dalším pomocníkem při kontrole řízeného vstupu jsou čipové karty pro vstup do jednotlivých pokojů, které v sobě zaznamenávají dobu vstupu. Provozní oddělení má pak možnost, pomocí čtečky karet, zpětně kontrolovat, která z přidělených karet k pokoji dveře otevřela a v kolik hodin. Počet karet, které jsou vydány odpovídá počtu ubytovaných hostů.

Systémy průmyslové televize

Díky kamerám, které monitorují hotelové a služební parkoviště, příjezdovou cestu a prostranství před garážemi, lze na recepci hotelu sledovat jakýkoliv pohyb na těchto prostranstvích.

Tento systém průmyslové televize slouží pouze k monitorování, signál není nikým ani ničím zaznamenáván, a ani není dostupný v hotelovém vysílání. Tím pádem se nejedná o narušení soukromí ubytovaných hostů, a není potřeba hosty podrobněji informovat o tomto systému zabezpečení, který se do určité míry vztahuje k ochraně osobních údajů podle zákona č. 101/2000 Sb.

Mechanické zábranné systémy

Tyto systémy řeší problematiku, jak odpovídajícím způsobem zabránit násilnému vniknutí osob do chráněného prostoru a následnému znehodnocení, narušení a poškození technického zařízení chráněného prostoru či odcizení citlivých údajů a důležitých dokumentů.

V organizaci se proti krádeži informací, dat a předmětů brání tím, že používají několik typů mechanických zábranných systémů:

Části vnějšího uzavření objektu

Pozemek hotelu je ohraničen železným a živým plotem, pro zabezpečení hotelového parkoviště je používána posuvná závora a plot tvořený zabetonovanými železnými sloupky.

Stavební prvky budov

Některé důležité místnosti jsou vybaveny nehořlavým sádrokartonem s protipožární úpravou.

Otvorové výplně budov

Na oknech provozního oddělení a skladovacích prostor hotelu, a na dveřích služebního vchodu jsou umístěny železné mříže bránící neoprávněnému vstupu do objektu.

Úschovné objekty

Funkci úschovných objektů plní v Parkhotelu Golf Mariánské Lázně, a. s. trezory a trezorové skříně, pokladny a kovové skříně.

Jedna trezorová skříň je umístěna na ekonomickém oddělení, druhá na recepci hotelu. Na provozním oddělení jsou zabudovány vestavěné trezory k uchovávání tiskopisů a datových zdrojů. Podobné trezory se také nacházejí na každém z pokojů hotelu.

Ekonomické oddělení má povinnost uchovávat údaje a výkazy o hospodaření společnosti v uzamykatelných kovových skříních.

Technické elektrické zabezpečení

Elektrická požární signalizace (EPS)

Toto zařízení sloužící k preventivní ochraně objektů před požárem není nainstalováno ve všech prostorech hotelu, nýbrž pouze na chodbách jednotlivých podlaží. Jedná se o čidla a hlásiče výskytu vzniku požáru.

Elektrická zabezpečovací signalizace (EZS)

Elektrická zabezpečovací signalizace sloužící k identifikaci narušení objektu není v hotelu nainstalována.

5. ZÁVĚR

Zabezpečení elektronických informací, dat a údajů by se mělo stát součástí aktivit každé organizace. Ne všechny organizace však realizují informační bezpečnost efektivně a komplexně. V praxi se můžeme setkat s tím, že bezpečnostní opatření jsou v organizacích aplikována bez znalosti míry existujících rizik. Takový přístup vede k existenci nedostatečně zabezpečených míst, o kterých organizace mnohdy ani netuší.

Každý systém je specifický, slouží pro různé účely a musí splňovat konkrétní potřebné parametry vyplývající z potřeb jeho uživatelů a zaměstnanců. Na každý systém jsou kladeny konkrétní bezpečnostní požadavky, z tohoto důvodu nelze obecně přejímat jednotlivé bezpečnostní koncepce a jednotlivá bezpečnostní opatření.

Organizace, kterou jsem si pro potřeby diplomové práce zvolil, je zařízením cestovního ruchu – hotel Parkhotel Golf Mariánské Lázně, a. s. Hotel zpracovává o svých klientech tyto citlivé údaje: jméno, příjmení, bydliště, datum narození, číslo průkazu totožnosti, národnost a zdravotní stav.

Jak již bylo zmíněno v druhé kapitole, statistiky dokládají, že zneužití informačního systému často bývá provedeno vlastními zaměstnanci organizace. Zabezpečením daného systému se organizace snaží minimalizovat možnost krádeží a pokusů o zneužití citlivých údajů, kterými jsou údaje o ubytovaných hostech a údaje o hospodaření společnosti.

Řešení informační bezpečnosti vyžaduje aktivní účast všech pracovišť a zaměstnanců hotelu, kteří se podílejí na zacházení s citlivými údaji a jejich zpracování. Některá rizika nelze úplně odstranit, ale je možnost je minimalizovat. Na druhou stranu může Parkhotel Golf Mariánské Lázně, a. s. jiná rizika akceptovat a nepřijímat vůči nim žádná opatření. Důležité však je, aby byla rizika identifikována a organizace věděla, že existují.

Při každodenní praxi není vždy možné striktně dodržet doporučené postupy a pravidla při zpracovávání citlivých údajů, je však ale potřeba aktivně přistupovat k řešení bezpečnostní problematiky na základě doporučených a ověřených postupů.

Nyní bych rád zhodnotil jednotlivé body bezpečnostní politiky.

V rámci fyzické bezpečnosti je ochrana před neoprávněným přístupem na prostranství hotelového parkoviště na vysoké úrovni. Vhodně umístěné sloupky spolu s posuvnou

závorou zamezují neoprávněnému přístupu automobilem. Jako nebezpečí ale shledávám omezené zorné pole kamery č. 4, která nemonitoruje služební vchod do budovy. Tento problém by se dal vyřešit usazením této kamery na pohyblivý kloub, čímž by kamera kontrolovala celý prostor služebního parkoviště, příjezdové cesty na služební parkoviště i prostranství před garážemi. Dále by měl hotel zvážit, zda nezvýšit počet kamer a některými z nich nesledovat např. bránu ústící na pozemek hotelu nebo prostranství před vstupem do hotelu.

Server byl z místnosti v 1. podzemním patře přemístěn do 3. nadzemního patra. Stalo se tak díky plánované přístavbě ubytovací části hotelu, kdy je lepší síťové kabely nejprve vést půdními prostory a poté je spouštět k jednotlivým oddělením dolů, než-li postupovat v opačném směru. Toto řešení je zároveň i ochranou proti případnému zaplavení podzemních místností a jeví se jako velice praktické.

U zabezpečení recepce se vyskytuje problém, jak ji vhodně zabezpečit v případě, že její zaměstnanec musí na určitou chvíli tento prostor opustit (toaleta, vyřešit problémy hostů na jejich pokoji, atd.). Jediným možným řešením, jak eliminovat riziko odcizení jakýchkoliv informací, dat a údajů je odhlášení se ze systému a uzamčení trezoru a trezorové skříně s tím, že klíč si odnáší s sebou. Vzhledem k architektonickému řešení prostor recepce není možné zcela vyloučit rizika spojená s ochranou citlivých údajů na tomto pracovišti.

Jeden z největších nedostatků ochrany dat jsem zjistil v prostorách provozního oddělení. Při opuštění pracoviště nedochází k uzamčení dveří provozních místností. Jelikož se zde nacházejí materiály obsahující citlivé údaje nejen o ubytovaných hostech, ale i např. o dodavatelích, pokládám za nutnost zabezpečit tyto místnosti proti možnosti neoprávněného vniknutí nainstalováním systému pro vstup pomocí kartového systému.

Ordinace a místnost vrchní sestry jsou z pohledu citlivých údajů zabezpečeny velice dobře. Pro zvýšení bezpečnosti proti neoprávněnému vniknutí bych doporučil nalepit do oken bezpečnostních fólie.

U fyzického zabezpečení ekonomického oddělení je problém kontroly zadního traktu hotelu ve večerních hodinách, kde se ekonomické oddělení nachází. Neexistuje zde žádná možnost, jak tyto prostory kontrolovat. Proto navrhuji místnost zabezpečit dveřmi s bezpečnostním kováním.

U zabezpečení archivu tiskopisů a elektronických médií jsem neshledal žádný problém.

Standardní ochranou **personální bezpečnosti** všech pracovišť je zákaz instalování vlastních programů a zákaz změny nastavení počítače. Velice vhodným bezpečnostním opatřením recepce shledávám přidělování uživatelských jmen a hesel až během zkušební doby, kterým se organizace chrání před odcizením citlivých údajů.

Na provozním a ekonomickém oddělení se jeví problém s přidělováním hesel pro přihlášení k počítači. Přihlášení k systému zde není realizováno prostřednictvím uživatelských účtů, zaměstnanec pouze zadává heslo pro přístup k počítači. Proto musí provozní oddělení vždy při ukončení pracovního poměru s příslušným zaměstnancem změnit přístupová hesla k danému počítači na konkrétním pracovišti. Tento problém je z části vyřešen díky velice malé fluktuaci zaměstnanců hotelu.

Na zdravotnickém oddělení jsou nároky na zabezpečení citlivých údaji vyšší, jelikož se zde zpracovávají údaje o zdravotním stavu pacientů a toto oddělení podléhá lékařskému tajemství. I přes vyšší nároky na bezpečnost hodnotím ochranu citlivých údajů na tomto pracovišti jako velmi dobrou.

Po datové stránce je zabezpečení organizace na velmi vysoké úrovni. Citlivé údaje o hotelových hostech mohou zadávat, upravovat a mazat pouze zaměstnanci recepce, citlivé údaje o hospodaření společnosti mohou zadávat, upravovat a mazat pouze zaměstnanci ekonomického oddělení a lékař upravuje pouze údaje týkající se zdravotního stavu hostů. To je důvodem, proč jsou údaje o zdravotním stavu hostů ukládány na pevný disk počítače a ne na disk serveru. Ostatní zaměstnanci, kteří jsou s citlivými údaji v kontaktu, mohou tyto údaje sledovat pouze v omezeném rozsahu.

Pro ochranu elektronických informací, dat a údajů je **z hlediska technické bezpečnosti** na každém počítači pravidelně prováděna aktualizace verzí programů. Pro modernizaci hardwarového vybavení jednotlivých oddělení má hotel zpracován plán obnovy.

Zálohování se nejčastěji provádí na média CD-R, a to z důvodu potřeby relativně malého množství dat, které je ukládáno – chorobopis jednoho pacienta má v průměru okolo 30 kB. Ekonomické oddělení pravidelně zálohuje na 3,5‘‘ diskety. Problém zde vidím v možnosti snadného mechanického poškození daného zálohovacího média.

Vhodným řešením ochrany dat na recepci hotelu je nepřítomnost zálohovací mechaniky CD±RW. Nicméně v současné době by se měl řešit problém s možností kopírovat či přesunout údaje na externí paměťová média, např. USB flash disk. Tento

problém by se mohl řešit pomocí nastavení příslušného počítače v rámci uživatelského účtu.

Zálohování na média DVD zatím není v organizace rozšířené z důvodu malého objemu zálohovaných dat.

Režimová bezpečnost hotelu je tvořena administrativními opatřeními a nařízeními, kterými jsou vnitřní směrnice a pokyny hotelu, etický kodex hotelu a bezpečnost práce na pracovišti. Podle dostupných zjištění mohu konstatovat, že směrnice a pokyny jsou striktně dodržovány na všech pracovištích hotelu. Systém kontrol je částečně zmíněn v systému managementu jakosti, který mimo jiné definuje pravidla pro provozování výpočetní techniky a programového vybavení, archivní a spisový řád.

Zaměstnanec, který má přístupové právo do systému, programu nebo k datům umístěných v počítačové síti hotelu pod heslem, musí o heslu zachovávat mlčenlivost, nesmí jej sdělovat dalším pracovníkům a je povinen se přihlašovat pouze pod tímto heslem. Je výslovně zakázáno sdělovat přístupová hesla spolupracovníkům, nebo příbuzným. V minulosti se zde objevoval problém s porušováním tohoto nařízení, např. u zaměstnanců recepce. V současné době, i díky systém zaznamenávajícího činnosti přihlášeného uživatele, které jsou ukládány na server, si zaměstnanci přístupy k uživatelským účtům nesdělují.

Velikou výhodu vidím v popisování jednotlivých písemností a elektronických médií v archivu hotelu.

Podle mého názoru je pro hotel **z hlediska komunikační bezpečnosti** výhodné zapojení počítačů do hvězdicové topologie. Výpadek jednoho z počítačů nemá vliv na funkčnost sítě, což je velice důležité pro organizaci, která pracuje s údaji uloženými na serveru každý den. Velice zajímavé a praktické řešení je, že při výpadku serveru nelze používat programy pracující s daty uloženými na serveru.

Jak již bylo zmíněno dříve, důležitým krokem zabezpečení proti zneužití údajů je sledování jednotlivých činností přihlášeného uživatele. Jeho činnosti a operace se zapisují do souboru na disk serveru a jsou snadno dohledatelné.

Parkhotel Golf Mariánské Lázně, a. s. nevyužívá při ukládání dat žádné kryptografické klíče, což se v budoucím vývoji informačních technologií jeví jako možná hrozba. Proto by stálo za zvážení, zda do budoucna nezvolit nějaký systém šifrování.

Hotel se nezabývá problematikou **procesního řízení bezpečnosti**. Domnívá se, že základní otázky týkající se ochranou údajů jsou součástí systému managementu jakosti ISO 9001:2000. Podle mého doporučení by si hotel měl nechat vypracovat alespoň jednu zprávu o procesním řízení bezpečnosti, například až se bude realizovat plánovaná přístavba ubytovací části hotelu a s tím související rozšíření počítačové sítě i do této části hotelu.

Hotel nevyužívá žádného elektrického **zařízení řízeného vstupu a pohybu**, jelikož tuto činnost plní zaměstnanci hotelu. Ti po dobu 24 hodin dohlížejí na pohyb hostů a osob v budově hotelu i mimo ni. Pohyb mimo budovu sledují 4 kamery umístěné na parkovištích hotelu, které ovšem tento signál nezaznamenávají. Ten je pouze sledován zaměstnanci recepce.

Z důvodu zvýšení bezpečnosti doporučuji tento signál zaznamenávat a archivovat. Tím ale vznikne povinnost řídit se různými zákony, např. zákonem č. 101/2000 Sb., o ochraně osobních údajů, protože z obrazu bude možno rozeznat jednotlivé osoby a podobizna je definována jako citlivý osobní údaj. Tím pádem nastane problém s informováním ubytovaných hostů o tomto kamerovém systému.

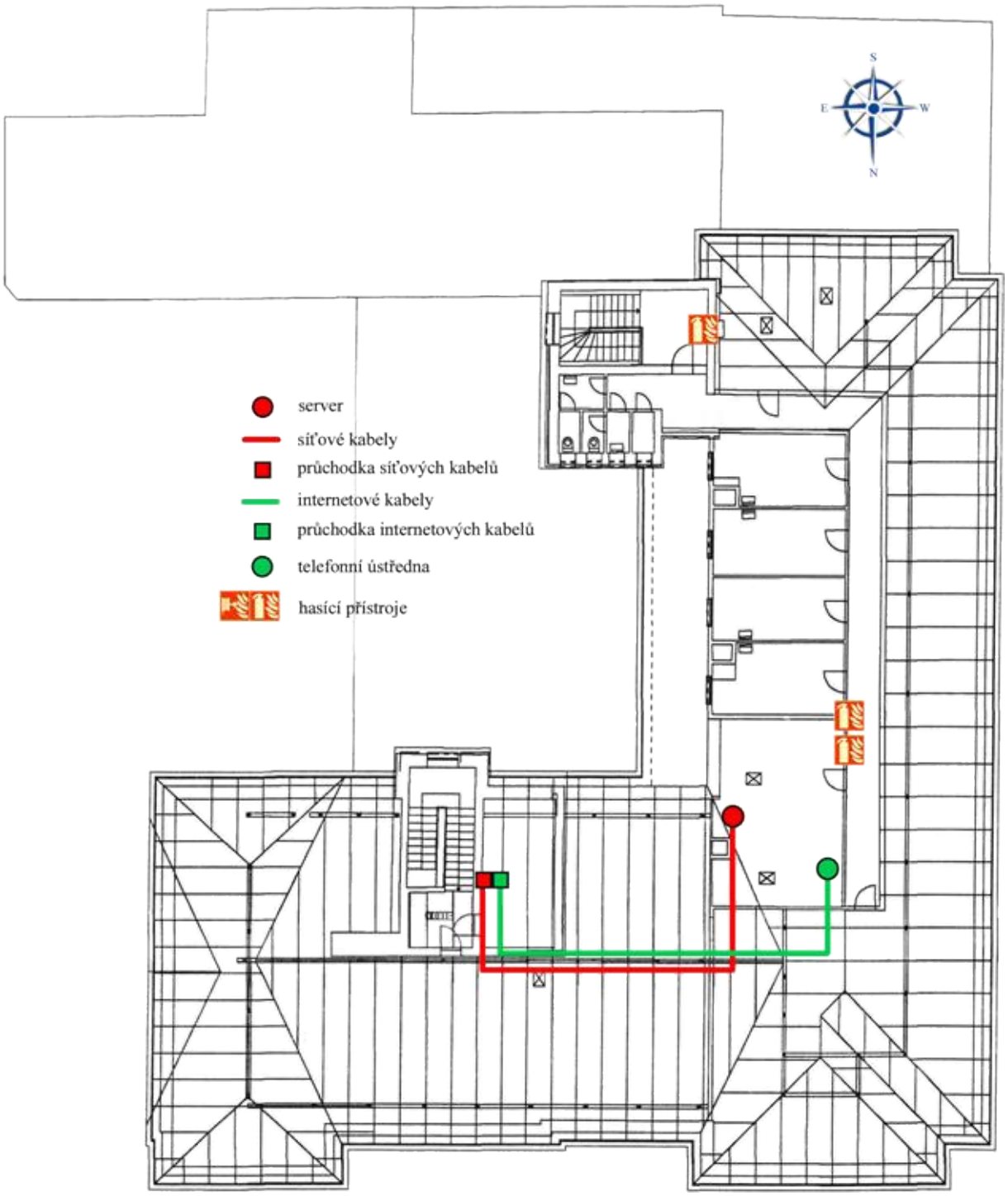
Pomocníkem při **monitorování vstupu** do pokojů jsou čipové karty, které zaznamenávají dobu vstupu. Provozní oddělení má možnost pomocí čtečky karet zpětně kontrolovat, která z přidělených karet dveře do pokoje otevřela a v kolik hodin.

Myslím si, že zabezpečení citlivých údajů z hlediska **použití mechanických zábranných systému** je řešeno velice dobře. K zabezpečení parkovišť slouží zabetonované železné sloupky a posuvná brána, v oknech jsou zabudovány mříže, u důležitých místností jsou použity bezpečnostní dveře. K uložení citlivých údajů se používají trezory a trezorové skříně, na některých odděleních se můžeme setkat i s železnými skříněmi.

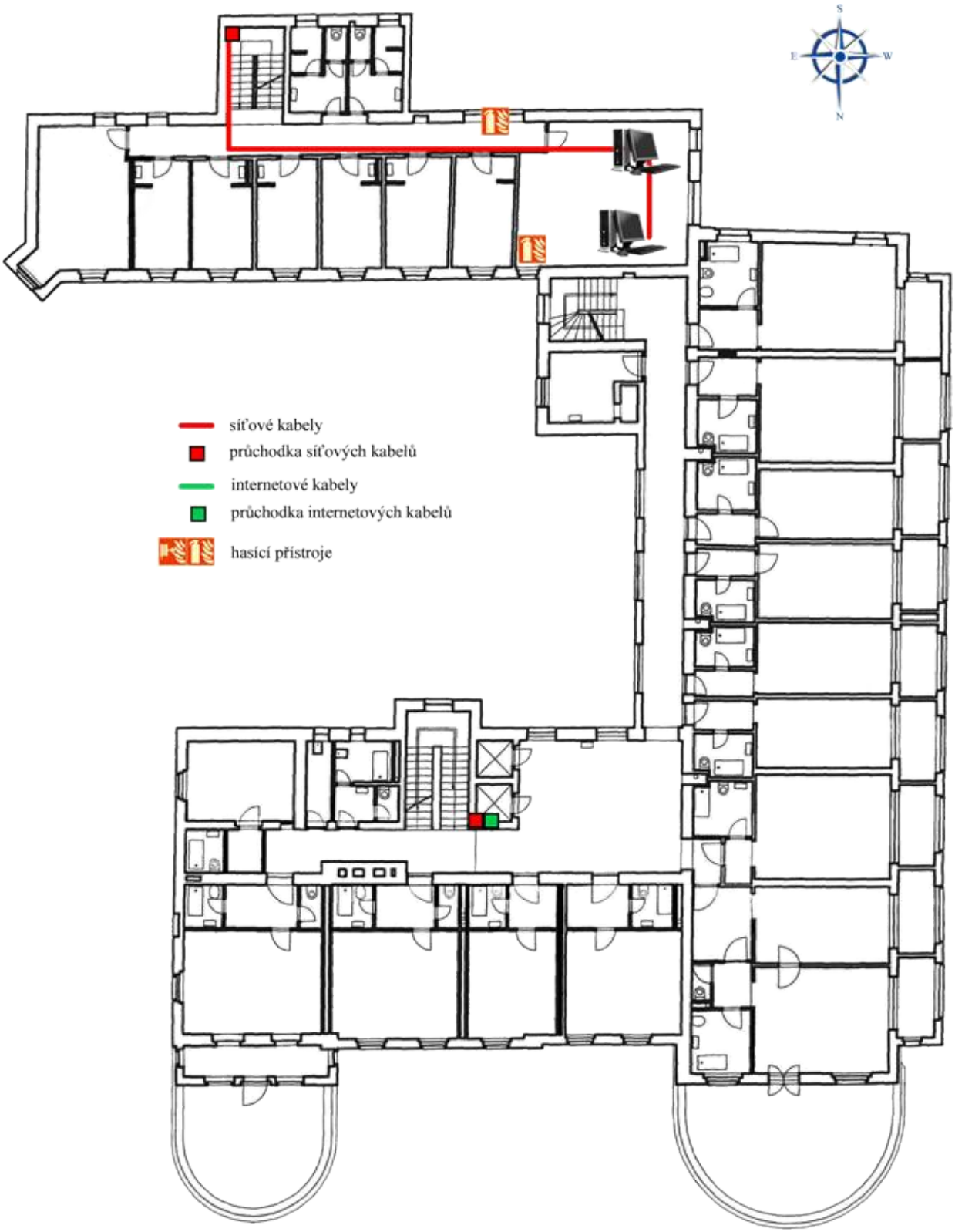
V této diplomové práci jsem se snažil popsat a zanalyzovat způsoby zabezpečení citlivých údajů a poskytnout celkový pohled na zabezpečení elektronických informací hotelu Parkhotel Golf Mariánské Lázně, a. s. Předpokládám, že přijme-li hotel alespoň některá z uvedených návrhů řešení, zvýší bezpečnost při zacházení s citlivými údaji.

SEZNAM PŘÍLOH

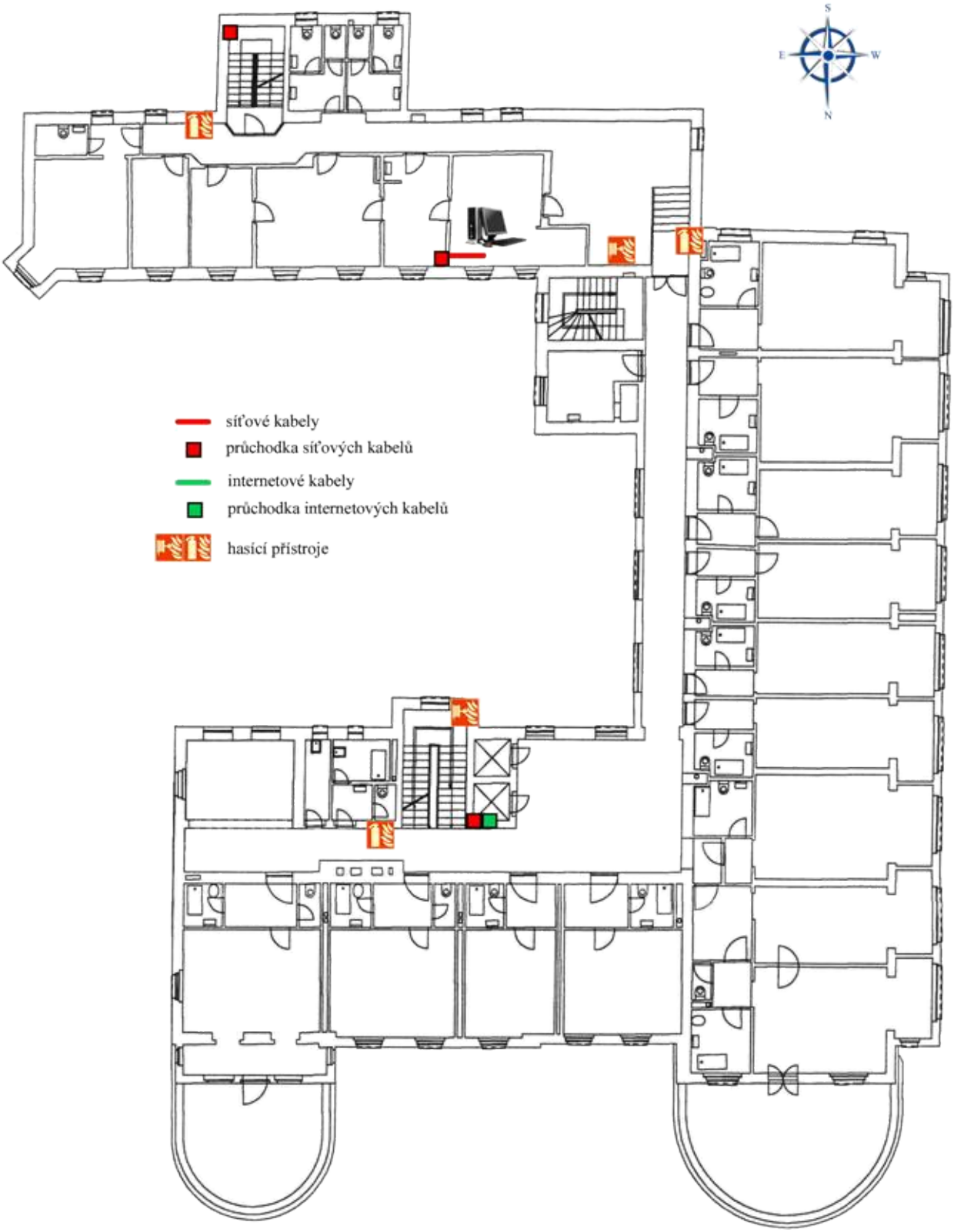
Příloha č. 1: Půdorys 3. nadzemního patra



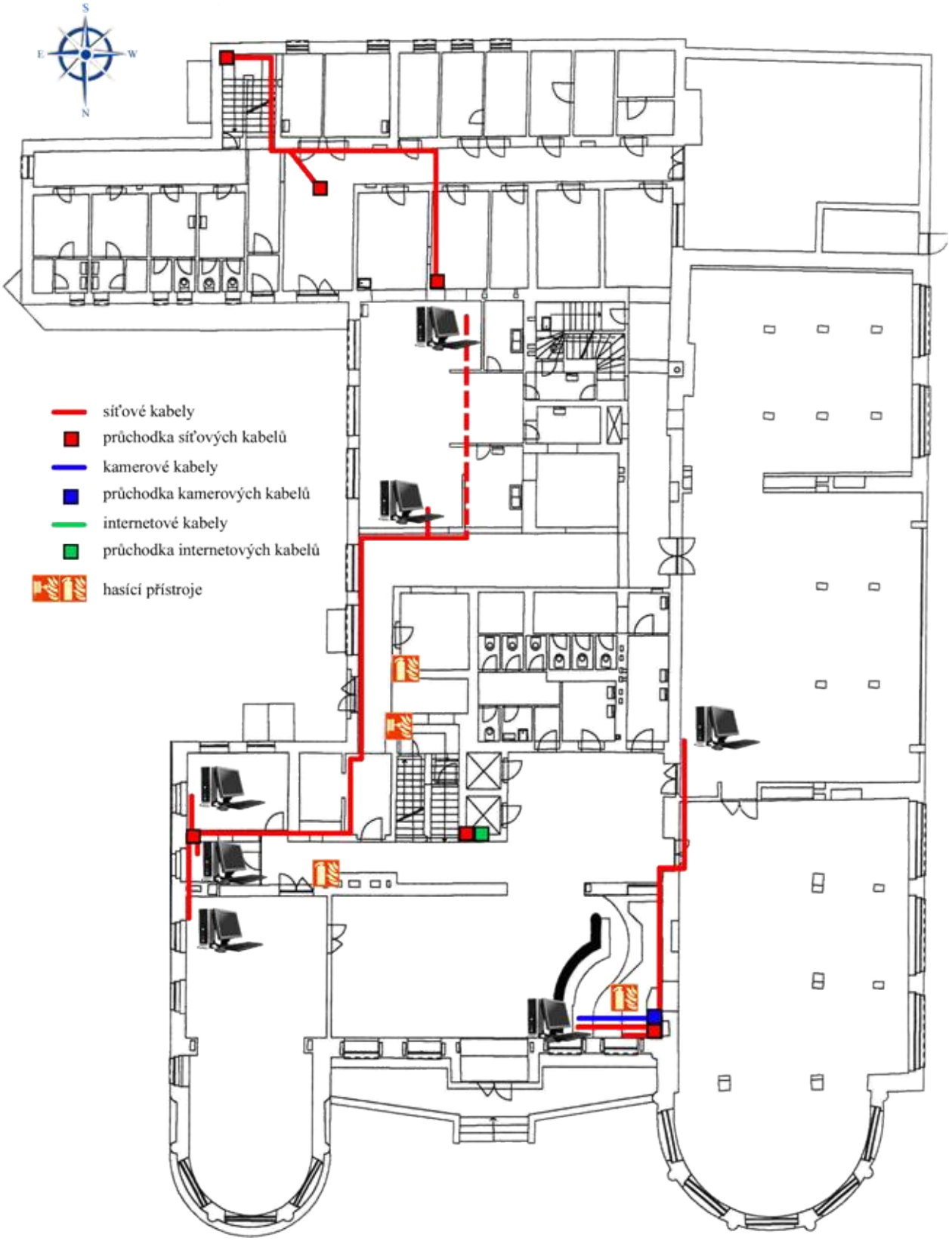
Příloha č. 2: Půdorys 2. nadzemního patra



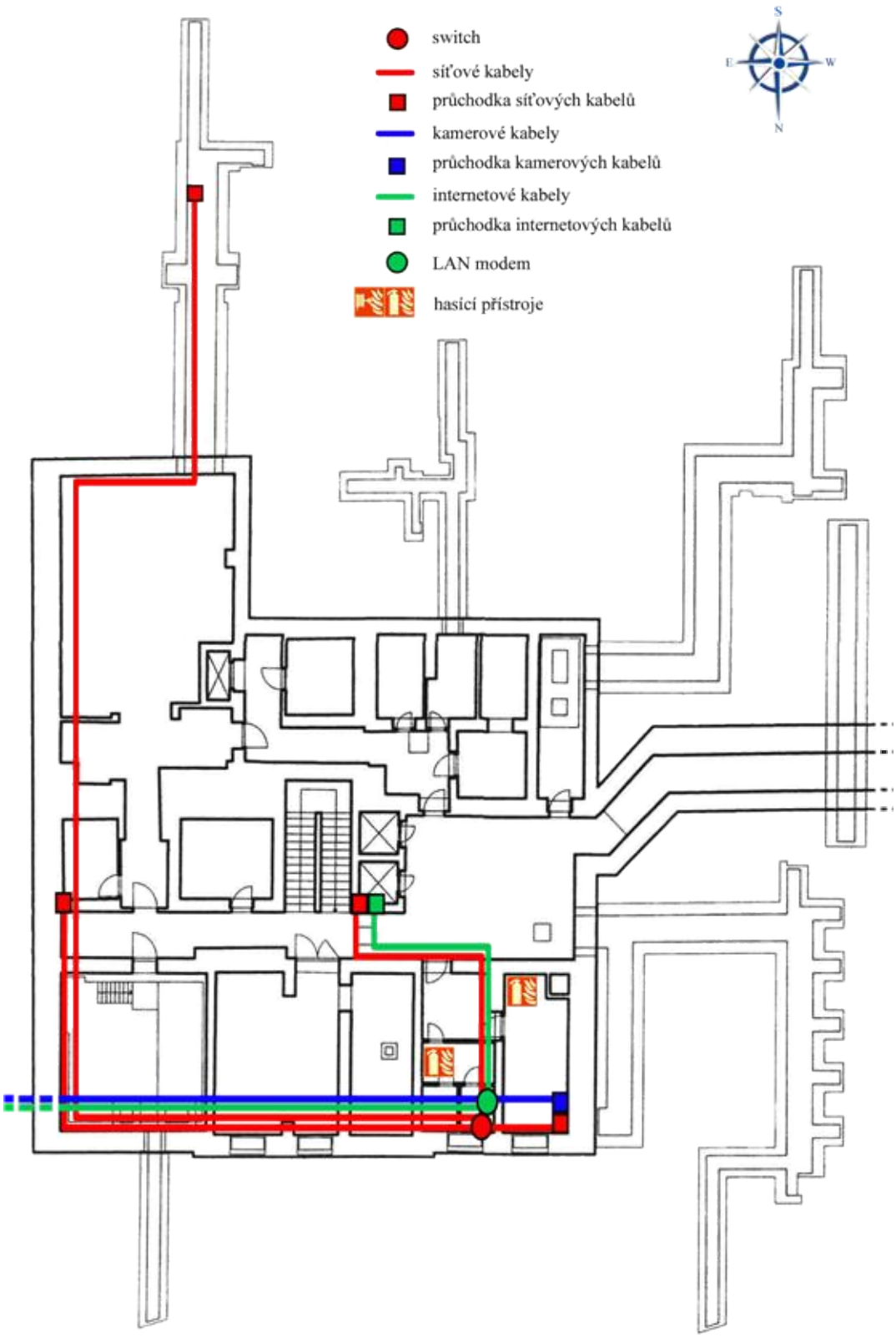
Příloha č. 3: Půdorys 1. nadzemního patra



Příloha č. 4: Půdorys přízemního patra



Příloha č. 5: Půdorys 1. podzemního patra



Příloha č. 6: Půdorys pozemku hotelu