Zajištění provozu multifunkčních, multimediálních elektronických zařízení určených pro zpracování utajovaných informací

Multifunkční, multimediální zařízení

- **Multimédia** jsou kombinace textu, audia, obrázků, animací, videa ve formě datových souborů zpracovávaných digitálně a ukládaných do paměti.
- **Multifunkční zařízení** (MFD - Multi-Function Device) nebo také „all-in-one“ zařízení sdružují více funkcí v jednou zařízení např.

  skenování + kopírování + tisk**.**

Charakteristické vlastnosti MFD

- digitální zpracování multimediálních datových souborů
- decentralizované zpracování, více výpočetních jednotek v zařízení
- masívní použití velkokapacitních paměťových medii (HD, SSD, paměťové karty) pro ukládání zpracovávaných dat (i několik HD v zařízení)
- vstup/výstup dat na přenosná paměťová media a prostřednictvím USB portů (flash disky, paměťové karty apod)
- rozsáhlá konektivita (Ethernet, WiFi, Bluetooth apod.)
- dostupnost, jednoduchá obsluha

Bezpečnostní rizika a hrozby

Nedostatky organizace provozu zařízení:

- Nedostatečné nebo špatné aplikování generických bezpečnostních požadavků, jejich kontroly a aktualizace
- Narušení fyzické bezpečnosti, nepovolený přístup k zařízení
- Možnost nekontrolovaného používání zařízení
- Problémy vyvolané absencí spotřebních materiálů a náplní (kopírka –papír, toner)
- Multifunkčnost sebou nese vyšší nároky bezpečnost (provázanost a závislost jednotlivých funkcí)

Lidské chyby:

- Ztráta důvěrnosti a integrity dat v důsledku chyb užívatelů a obsluhy (ponechání dat v zařízení, zápis dat na nesprávný nosič apod.)
- Porušování nebo ignorování bezpečnostních požadavků (nechrání se přístupová hesla, nedodržování postupu pro vypínání zařízení apod.)
- Problémy způsobené úklidovým personálem a jinými návštěvníky

Bezpečnostní rizika a hrozby

Technická selhání

- Nedokumentované funkce zařízení – mohou a nemusí způsobovat problémy
- Multifunkčnost + dálková správa + nešifrovaná komunikace = zdroj bezpečnostních rizik

Úmyslná narušení bezpečnosti

- Průnik do zařízení s cílem odcizení dat nebo destrukce zařízení
- Narušení důvěrnosti kopírováním/čtením dat, odezíráním displeje, odcizením vstupně výstupních dat
- **Využití zbytkové informace v paměťi vestavěné v zařízení**

  V zařízení jsou dva druhy pamětí :

  1. obsah se vymaže vypnutím napájení (volatile [volata:il] storage) např. operační paměť
  2. obsah se uchová i po vypnutí napájení (non-volatile storage) např. harddisk

Závěr

Hlavní nepřátelé bezpečnosti jsou člověk + konektivita + paměťové nosiče informací !

Bezpečnostní rizika a hrozby

Mobilizující reportáž televize CBS odvysílaná 19.4.2010 :
CBS News: Copy Machines, a Security Risk?
http://www.youtube.com/watch?v=y01xLquSIrc

Bezpečnost MFD zajištěná výrobcem

- Každý **renomovaný** výrobce má zpracovaný manuál k produktu nebo řadě produktů popisující bezpečnostní parametry zařízení
- Některé výrobky jsou certifikovány např podle normy ISO/IEC 15408 (Common Criteria)
- Dokumenty jsou v otevřeném tvaru zpracovávané pouze v operační paměti
- Ochrana hardisku : šifrování, automatický přepis dat, destrukce FAT tabulky a přeformátování apod.
- Při zapnutí MFD probíhá kontrola validity firmware pomocí HW obvodu TPM (Trusted Platform Module)
- Různé varianty autentizace a autorizace uživatelů
- Audit a monitorování činnosti

Zpracování utajovaných informací

Zákon 412/2005 Sb.,§ 36

Ochrana utajovaných informací v kopírovacím zařízení, zobrazovacím zařízení nebo psacím stroji s pamětí (dále jen zařízení)

- chráněná utajovaná informace je v elektronické podobě
- zpracování probíhá v kopírovacím, zobrazovacím zařízení nebo psacím stroji s pamětí, které nejsou součástí informačního nebo komunikačního systému
- orgán státu, právnická osoba a podnikající fyzická osoba jsou povinni zpracovat bezpečnostní provozní směrnici a zpracovávat utajované informace pouze v souladu s touto směrnicí,
- bezpečnostní provozní směrnice musí obsahovat : způsob provozování zařízení a provozní směrnici uživatele zařízení

Vyhláška č.523, § 38

Podmínky bezpečného provozování kopírovacího zařízení, zobrazovacího zařízení nebo psacího stroje s pamětí

V závislosti na stupni utajení utajovaných informací se uplatňuje soubor opatření z oblasti :

a) personální bezpečnosti,
b) fyzické bezpečnosti,
c) administrativní bezpečnosti a organizačních opatření
d) ochrany utajované informace před jejím únikem kompromitujícím elektromagnetickým vyzařováním.

- Zařízení, které se používají pro zpracování utajovaných informací stupně utajení Důvěrné nebo vyššího, **musí být zabezpečeny proti úniku utajované informace kompromitujícím elektromagnetickým vyzařováním.**
- Zařízení, **musí být umístěny do prostoru, ve kterém je zajištěna jejich fyzická ochrana před neoprávněným přístupem, poškozením a ovlivněním.** Tento prostor je vymezen definovanými prvky ochrany s vhodnými kontrolami vstupu a bezpečnostními bariérami. Podle charakteru zařízení se na základě analýzy rizik stanovuje, zda musí být umístěno v zabezpečené oblasti nebo v objektu, a požadovaná kategorie zabezpečené oblasti.
- Zařízení, **musí být fyzicky chráněny před bezpečnostními hrozbami a riziky prostředí.**
- Umístění Zařízení, musí být provedeno tak, aby **zamezovalo nepovolané osobě odezírat utajované informace.**
- **Se zařízením obsahujícím zabudované nosiče utajovaných informací nebo jiné komponenty umožňující uchování utajovaných informací musí být spojena informace o stupni utajení informací uchovávaných na těchto nosičích, komponentách a pamětech.** Tato informace může být vyjádřena na štítku připevněném k zařízení, stanovena v bezpečnostní provozní směrnici nebo být vyjádřena jiným vhodným způsobem. Nosiče utajovaných informací zabudované do zařízení a jiné komponenty umožňující uchování utajovaných informací musí být evidovány a označeny stupněm utajení nejpozději po jejich vyjmutí z daného zařízení.
- **Servisní činnost pro kopírovací zařízení, zobrazovací zařízení a psací stroje s pamětí se musí organizovat tak, aby nebyla ohrožena bezpečnost utajovaných informací. Z nosičů utajovaných informací a pamětí přístupných při servisní činnosti musí být vymazány utajované informace.**

MV ČR

- MFD pro stupně utajení V, D, T
- omezený počet zařízení, pozvolná inovace, decentralizované pořízení a nákup
- Problematiku řeší „**Pokyn ministra vnitra č. 54 k ochraně utajovaných informací v kopírovacím zařízení, zobrazovacím zařízení nebo psacím stroji s pamětí**“, který
  1. obsahuje bezpečnostní provozní směrnici zařízení, vzor pro zpracování bezpečnostní směrnice uživatele a vzor provozního deníku
  2. ukládá vedoucím pracovníkům MV a PČR předkládat bezpečnostnímu řediteli MV (řediteli BO) údaje k zařízením, která navrhují k použití pro zpracovávání utajovaných informací a zabezpečit realizaci bezpečnostní provozní směrnice zařízení
  3. ukládá řediteli BO stanovit provozní směrnici uživatele konkrétního zařízení, zajišťovat u NBÚ ověření způsobilosti zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajovaných informací KEV, provádět kontrolu dodržování pokynu.

MV ČR

Bezpečnostní provozní směrnice zařízení pro zpracovávání utajovaných informací

- **Používání zařízení schvaluje příslušný vedoucí funkcionář útvaru** (dále jen „ředitel“) v provozním deníku zařízení
- Ředitel **stanoví pověřenou osobu** odpovědnou za provoz zařízení a vedení provozního deníku (dále jen „pověřená osoba“).
- **Pro každé zařízení se zpracovává provozní směrnice uživatele**. Zpracovává ji BO na základě údajů poskytnutých ředitelem.
- **Zařízení musí být na viditelném místě označeno** (spisová značka útvaru a evidenční číslo zařízení, pod kterým je vedeno v Provozním deníku. U zařízení se zabudovaným nosičem se uvede i nejvyšší stupeň utajení zpracovávaných informací.
- Nosič informací, na který lze ukládat utajovanou informaci a který lze do zařízení opakovaně vložit a vyjmout, např. video kazeta, paměťová karta, páska do psacího stroje apod.(dále jen „**vyměnitelný nosič**“), se před prvním uložením utajované informace označuje jako utajovaný dokument v nelistinné podobě
- Nosič informací, na který lze ukládat utajovanou informaci a který nelze do elektronického zařízení opakovaně vložit a vyjmout bez použití dalších nástrojů, např. nevyjímatelný pevný disk apod., (dále jen „**zabudovaný nosič**“), musí být evidován stejným způsobem jako vyměnitelný nosič a označuje se neprodleně po jeho prvním vyjmutí ze zařízení.

MV ČR

- zařízení se při provozování umísťuje nebo zajišťuje tak, aby neoprávněná osoba neměla samostatný přístup k zařízení a nemohla odezírat zpracovávané utajované informace. Konkrétní umístění a zajištění se stanoví v provozní směrnici uživatele.
- Nepřenositelné zařízení se zabudovaným nosičem, ze kterého nelze vymazat utajovanou informaci, se provozuje pouze v zabezpečené oblasti, jejíž kategorie odpovídá stejnému nebo vyššímu stupni utajení zpracovávaných utajovaných informací.
- Přenosné zařízení se provozuje v zabezpečené oblasti nebo v objektu. V odůvodněných případech může být provozováno s písemným souhlasem ministra vnitra nebo bezpečnostního ředitele i mimo objekt
- Přenosné elektronické zařízení se zabudovaným nosičem se ukládá do úschovného objektu v zabezpečené oblasti nebo do zabezpečené oblasti, jejíž kategorie odpovídá stejnému nebo vyššímu stupni jeho utajení
- **KEV**
- zařízení je oprávněna používat osoba, které je umožněn přístup k utajované informaci, byla prokazatelně seznámena s obsluhou zařízení a s provozní směrnicí uživatele (dále jen „uživatel“).

MV ČR

- zařízení s nosičem pro ukládání utajovaných informací stupně utajení D lze přenášet se souhlasem ředitele.
- zařízení s nosičem pro ukládání utajovaných informací stupně utajení T a PT lze přenášet s písemným souhlasem ředitele.
- Opravu a servisní prohlídku zařízení a jeho přípravu k opravě a servisní prohlídce zajišťuje pověřená osoba.
- Před opravou nebo servisní prohlídkou zařízení se zabudovaným nosičem, ze kterého lze vymazat informaci se utajované informace vymažou způsobem stanoveným v provozní směrnici uživatele.
- Ukončení používání zařízení schvaluje svým podpisem ředitel a zaznamenává to v provozním deníku.
- zařízení se zabudovaným nosičem nelze po ukončení používání dále používat bez kvalifikovaného vymazání informací z nosiče, které zamezí získání zbytkové utajované informace z nosiče nebo vyjmutí zabudovaného nosiče.
- Dokumenty zpracované k provozu zařízení se ukládají po dobu 5 let od ukončení jeho používání.

Provozní deník

„Provozní deník“

Vnitřní desky:

Evidence elektronických zařízení

ev. č.	název elektronického zařízení	typové označení	výrobní číslo	nejvyšší stupeň utajení zprac. informací	datum určení ke zprac. UI a podpis ředitele	datum ukončení určení ke zprac. UI a podpis ředitele
1	kopírovací stroj	KTC 22	00098765432	Tajné	2. 2. 2006 Štika	
2	videokamera	Panasonic RV7X	00002354678	Důvěrné	2. 2. 2006 Štika	

Provozní deník

Jednotlivé listy:

datum, čas od-do	ev. č.	záznam o závadě zařízení, jeho opravě a servisní činnosti	jméno, podpis
21. 7. 2006 8. 00-8. 30	2	čištění objektivu, servisní úkon provedl Jan Nový, OP č. 111111567, firma OKOUN	Vaněk

Provozní směrnice uživatele elektronického zařízení

název zařízení	kopírovací zařízení (Rxxxx AB 1111)
evidenční číslo zařízení	KOV16
umístění	PCR Albrechtova 2, Hradec Králové 1. NP – místnost č. 888
nejvyšší stupeň utajení zpracovávaných informací	Důvěrné
jméno osoby odpovědné za provoz zařízení	Jana Nová tel. 111 222

Při provozu je nutné zajistit splnění těchto požadavků:

1. kopírovací zařízení (dále jen „zařízení") se k síťovému přívodu připojuje přes síťový filtr s vypínačem a musí být umístěno nejméně x m od nefiltrovaných rozvodů elektrické sítě, slaboproudých metalických vedení (tel. rozvody, EPS, EZS atd.), rozvodů ústředního vytápění a dalších nefiltrovaných kovových částí v místnosti.
2. zařízení je oprávněna používat pouze osoba, které je umožněn přístup k utajované informaci, a která byla prokazatelně seznámena s obsluhou zařízení a provozní směrnicí uživatele. Je nutné zamezit nepovolenému přístupu k řídicí elektronice zařízení (např. páskovým pečetěním krycího panelu).
3. Před zrušením zařízení je nutné, aby autorizovaný servis provedl vyjmutí a protokolární předání paměťových nosičů (paměťových modulů, pevných disků apod.) osobě odpovědné za provoz zařízení, která zajistí jejich zničení.

Povinnosti uživatele:

Uživatel je při zpracovávání utajovaných informací v zařízení zejména povinen:

1. používat zařízení v souladu s jeho návodem k obsluze,
2. nepřemisťovat zařízení bez souhlasu osoby odpovědné za provoz zařízení,
3. nepřipojovat zařízení k elektronickým přístrojům, počítačovým a telefonním sítím,
4. oznámit neprodleně osobě odpovědné za provoz zařízení jakoukoli závadu, poruchu nebo nestandardní chování zařízení,
5. zamezit neoprávněné osobě přístup k zařízení nebo odezírání utajovaných informací,
6. nevzdalovat se od zařízení v průběhu zpracování utajovaných informací,
7. po ukončení zpracování utajovaných informací nejprve vypnout vypínač napájení na zařízení a následně vypínač na síťovém filtru nejméně na dobu 2 minut,
8. zkontrolovat před odchodem od zařízení, zda v zařízení nebo na manipulačních plochách u zařízení nezůstaly utajované informace.