HP Security Manager 3.16

Přehled 124 bezpečnostních Policy Items

Co dokument představuje
HP Security Manager umožňuje sestavit bezpečnostní politiku z jednotlivých kontrolních a konfiguračních pravidel. Tento přehled shrnuje 124 Policy Items dostupných v HP Security Manager 3.16.0.395 a stručně vysvětluje, co jednotlivé položky kontrolují nebo nastavují.

Poznámka k rizikům: uvedené riziko je stručná praktická interpretace dopadu daného nastavení. Nejde o pevně danou úroveň závažnosti od HP; skutečné riziko se vždy odvíjí od prostředí, využívaných funkcí a bezpečnostních požadavků organizace.

Přizpůsobitelná politika	Audit a vyhodnocení	Automatická náprava
Organizace si může vybrat jen ta pravidla, která odpovídají jejím bezpečnostním a provozním požadavkům.	HPSM porovnává skutečné nastavení zařízení s definovanou politikou a zvýrazňuje odchylky podle závažnosti.	U podporovaných položek lze povolit Remediation, tedy automatické uvedení nevyhovující konfigurace do požadovaného stavu.

Rozsah podle bezpečnostních oblastí

Authentication	Device Control	Device Discovery	Printing	Digital Services	Network Security	Network Services
24	41	5	12	11	11	20

Důležité: Dostupnost konkrétní položky, hodnot a možnosti automatické nápravy se mohou lišit podle modelu zařízení, firmware a aktivovaných funkcí. HPSM umí pro nepodporované položky definovat způsob vyhodnocení.

Authentication | 24 Policy Items

Řízení přístupu, přihlašovacích metod, hesel, SNMP a certifikátů.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
1	Authentication Manager	**Guest Access**	Určuje, zda mohou uživatelé bez přihlášení používat funkce zařízení.	Neoprávněné použití funkcí zařízení bez identifikace uživatele a horší dohledatelnost činností.
2	Authentication Manager	**Administrative Function Authentication**	Vyžaduje ověření uživatele před přístupem k administrativním funkcím zařízení.	Neoprávněná změna bezpečnostních nebo provozních nastavení zařízení.
3	Authentication Manager	**Job Storage Authentication**	Řídí, zda je pro ukládání a vyvolání uložených tiskových úloh nutné ověření.	Přístup cizí osoby k uloženým tiskovým úlohám nebo jejich neoprávněné vytištění.
4	Authentication Manager	**Print and Copy Authentication**	Řídí ověřování uživatele pro tiskové a kopírovací funkce zařízení.	Neautorizované používání tisku a kopírování a omezená odpovědnost za provedené operace.
5	Authentication Manager	**Digital Services Authentication**	Řídí ověřování pro digitální služby, například adresář, e-mail nebo fax.	Neoprávněné skenování, odesílání dokumentů nebo využití digitálních služeb.
6	Authentication Manager	**EWS Authentication**	Určuje, zda je pro přístup k funkcím Embedded Web Serveru vyžadováno ověření.	Neoprávněný přístup k webové správě zařízení a změnám konfigurace.
7	Credentials	**Admin (EWS) Password and Account Policy**	Kontroluje administrátorské heslo EWS a související pravidla délky, složitosti a blokace účtu.	Slabé nebo chybějící administrátorské heslo může vést k převzetí správy zařízení.
8	Credentials	**Microsoft Entra ID Sign-In Setup**	Kontroluje nastavení přihlašování k zařízení pomocí Microsoft Entra ID.	Nesprávné nastavení identity může umožnit chybnou autentizaci nebo blokovat oprávněné uživatele.
9	Credentials	**SNMPv1/v2**	Kontroluje stav SNMPv1/v2 a požadované Read/Write community names.	Nešifrované community strings mohou být odposlechnuty nebo zneužity ke čtení či změně konfigurace.
10	Credentials	**SNMPv3**	Kontroluje zapnutí a zabezpečení SNMPv3 včetně uživatele, autentizace a šifrování.	Slabé nebo chybné nastavení SNMPv3 snižuje ochranu správy zařízení proti odposlechu a zneužití.
11	Credentials	**File System Password**	Kontroluje heslo chránící přístup k souborovému systému zařízení.	Nechráněný souborový systém může umožnit přístup k uloženým souborům nebo konfiguraci.
12	Credentials	**PJL Password**	Kontroluje heslo používané k ochraně příkazů PJL.	Nechráněné PJL příkazy mohou umožnit změny nastavení nebo jiné privilegované operace.
13	Credentials	**Remote Configuration Password**	Kontroluje heslo pro vzdálenou konfiguraci zařízení.	Neoprávněná vzdálená konfigurace zařízení při kompromitaci nebo absenci hesla.
14	Credentials	**Bootloader Password**	Kontroluje heslo chránící přístup k bootloaderu zařízení.	Neoprávněný zásah do nízkoúrovňového spouštění zařízení nebo firmware.
15	Credentials	**Service Access Code**	Kontroluje servisní přístupový kód používaný pro privilegované servisní funkce.	Neoprávněný přístup k servisním funkcím a nastavením s vyššími oprávněními.
16	Credentials	**Group One PIN**	Kontroluje nastavení prvního skupinového PINu pro autentizaci uživatelů.	Sdílený nebo slabý PIN může umožnit neoprávněný přístup k funkcím přiřazeným skupině.
17	Credentials	**Group Two PIN**	Kontroluje nastavení druhého skupinového PINu pro autentizaci uživatelů.	Sdílený nebo slabý PIN může umožnit neoprávněný přístup k funkcím přiřazeným skupině.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
18	Credentials	**Fax PIN Presence**	Ověřuje, zda je pro faxové funkce nastaven požadovaný PIN.	Neoprávněné použití faxových funkcí nebo odesílání informací mimo organizaci.
19	Authentication Services	**802.1x Authentication (wired)**	Kontroluje 802.1X autentizaci zařízení na kabelové síti.	Zařízení se může připojit do kabelové sítě bez ověření identity a obejít síťovou kontrolu přístupu.
20	Authentication Services	**802.1x Authentication (wireless)**	Kontroluje 802.1X autentizaci zařízení na bezdrátové síti.	Zařízení se může připojit do bezdrátové sítě bez odpovídající autentizace.
21	Authentication Services	**LDAP Server Authentication**	Kontroluje použití LDAP serveru pro autentizaci uživatelů.	Chybné LDAP nastavení může vést k neoprávněnému přístupu nebo selhání ověření uživatelů.
22	Authentication Services	**SIP Server Settings**	Kontroluje nastavení SIP serveru používaného souvisejícími komunikačními funkcemi zařízení.	Nesprávná nebo nezabezpečená konfigurace SIP může vystavit komunikační funkce zneužití.
23	Certificate Management	**Identity Certificate**	Kontroluje identitní certifikát zařízení používaný pro jeho ověření a zabezpečenou komunikaci.	Neplatný nebo nedůvěryhodný certifikát umožňuje podvržení identity zařízení nebo chyby TLS.
24	Certificate Management	**CA Certificate**	Kontroluje důvěryhodné certifikáty certifikačních autorit uložené v zařízení.	Nesprávná sada důvěryhodných CA může umožnit důvěru podvrženým certifikátům nebo blokovat legitimní komunikaci.

Device Control | 41 Policy Items

Ochrana uložených dat, ovládacího panelu, fyzických rozhraní, firmware a interních bezpečnostních funkcí.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
25	Stored Data	**File Erase Mode**	Určuje způsob bezpečného mazání dočasných dat a souborů z úložiště zařízení.	Obnovení citlivých dat ze zařízení po smazání nebo vyřazení úlohy.
26	Stored Data	**RAM Disk Configuration**	Kontroluje konfiguraci RAM disku používaného pro dočasná data.	Nevhodné ukládání dočasných dat může zvýšit riziko jejich zpřístupnění nebo ztráty.
27	Stored Data	**Retain Print Jobs**	Řídí, zda a jak dlouho mohou být tiskové úlohy uchovány v zařízení.	Citlivé dokumenty mohou zůstat uložené v zařízení déle, než je nezbytné.
28	Stored Data	**Stored Data PIN Protection**	Kontroluje ochranu uložených dat a úloh pomocí PINu.	Uložené dokumenty mohou být vytištěny nebo zpřístupněny bez znalosti PINu.
29	Stored Data	**Retain Temporary Print Jobs After Reboot**	Určuje, zda dočasné tiskové úlohy zůstávají zachovány po restartu zařízení.	Dočasné úlohy mohou přetrvat restart a zůstat dostupné neoprávněným osobám.
30	Stored Data	**Temporary Job Storage Limit**	Omezuje množství prostoru vyhrazeného pro dočasně uložené úlohy.	Nadměrné ukládání úloh může prodloužit expozici dat a zaplnit úložiště zařízení.
31	Logging	**Syslog (System Logging)**	Kontroluje odesílání systémových a bezpečnostních událostí na Syslog server.	Bez centrálního logování se hůře odhalují incidenty a zpětně dohledávají změny či útoky.
32	Control Panel	**Control Panel (CP) Lock**	Kontroluje úroveň uzamčení ovládacího panelu proti neoprávněným změnám.	Lokální uživatel může změnit konfiguraci nebo bezpečnostní nastavení z ovládacího panelu.
33	Control Panel	**Control Panel Timeout**	Určuje dobu nečinnosti, po které ovládací panel automaticky ukončí relaci nebo se zamkne.	Opuštěná přihlášená relace může zůstat dostupná další osobě.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
34	Control Panel	**Display Job Status**	Řídí, jaké informace o tiskových úlohách jsou zobrazovány na ovládacím panelu.	Zobrazení názvů úloh či uživatelů může odhalovat citlivé informace.
35	Control Panel	**Control Panel Logout Policy**	Kontroluje pravidla automatického odhlášení uživatele z ovládacího panelu.	Uživatel může zůstat přihlášený déle, než je bezpečné, a umožnit zneužití relace.
36	External Connections	**Direct Connect Ports**	Kontroluje stav fyzických přímých komunikačních portů zařízení.	Nepotřebné fyzické porty mohou sloužit jako alternativní cesta k zařízení mimo standardní síťové kontroly.
37	External Connections	**Host USB Plug and Play**	Řídí možnost připojit USB zařízení přes Host USB Plug and Play.	USB zařízení může zavést neautorizovaný obsah nebo umožnit přenos dat mimo kontrolované kanály.
38	Device Security Checks	**Check for Latest Firmware and optional Firmware Security Assessment Reporting**	Ověřuje aktuálnost firmware zařízení a volitelně vyhodnocuje jeho bezpečnostní stav.	Neaktuální firmware může obsahovat známé zranitelnosti nebo chybějící bezpečnostní opravy.
39	Device Security Checks	**Check for Latest Jetdirect Firmware**	Kontroluje, zda je firmware síťového rozhraní HP Jetdirect aktuální.	Neaktuální síťový firmware může obsahovat zneužitelné chyby v komunikačních službách.
40	Device Security Checks	**Secure Boot Presence**	Ověřuje přítomnost a podporu Secure Boot pro ochranu spouštění důvěryhodného firmware.	Bez Secure Boot může zařízení spustit nedůvěryhodný nebo pozměněný firmware.
41	Device Security Checks	**Intrusion Detection Presence**	Ověřuje přítomnost funkce detekce narušení zařízení.	Bez detekce narušení může podezřelé chování zůstat bez povšimnutí.
42	Device Security Checks	**Whitelisting Presence**	Ověřuje přítomnost whitelisting funkce pro spouštění pouze důvěryhodného kódu.	Bez whitelisting kontroly může zařízení spustit nepovolený nebo pozměněný kód.
43	General	**Role Based Access Control**	Kontroluje používání řízení přístupu na základě rolí (RBAC).	Příliš široká oprávnění zvyšují riziko neoprávněného přístupu k funkcím a nastavením.
44	General	**Assign Roles to User and Group**	Kontroluje přiřazení definovaných rolí konkrétním uživatelům a skupinám.	Chybné přiřazení rolí může dát uživateli vyšší oprávnění, než potřebuje.
45	General	**Erase Data**	Kontroluje nastavení funkce pro vymazání dat uložených v zařízení.	Nesprávné nebo neúplné vymazání může ponechat citlivá data na zařízení.
46	General	**PJL Access Commands**	Řídí, které příkazy PJL zařízení přijímá a zpracovává.	Nadměrně povolené PJL příkazy mohou umožnit změnu konfigurace nebo přístup k interním funkcím.
47	General	**PostScript Security**	Kontroluje bezpečnostní omezení pro zpracování PostScriptu.	Neomezené PostScript operace mohou být zneužity k přístupu k funkcím nebo datům zařízení.
48	General	**Near Field Communication (NFC)**	Kontroluje zapnutí rozhraní Near Field Communication (NFC).	Aktivní NFC může vytvořit další lokální komunikační kanál bez potřeby organizace.
49	General	**Auto Send**	Kontroluje funkci AutoSend pro automatické odesílání informací o zařízení.	Automatické odesílání údajů může nechtěně předávat provozní či jiné informace mimo organizaci.
50	General	**Extended Signature Verification**	Kontroluje rozšířené ověřování digitálních podpisů firmware a kódu.	Nedostatečné ověření podpisu zvyšuje riziko spuštění pozměněného firmware nebo kódu.
51	General	**Wi-Fi Direct**	Kontroluje stav Wi-Fi Direct pro přímé bezdrátové připojení klientů k tiskárně.	Přímé bezdrátové připojení může obejít podnikové síťové řízení, segmentaci a autentizaci.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
52	General	**Wireless Direct Print**	Kontroluje funkci Wireless Direct Print pro přímý bezdrátový tisk.	Přímý bezdrátový tisk může umožnit tisk mimo standardní síťové a přístupové kontroly.
53	General	**Wireless Radio State**	Kontroluje, zda je bezdrátové rádio zařízení zapnuté nebo vypnuté podle politiky.	Zbytečně aktivní bezdrátové rádio rozšiřuje útočnou plochu a možnosti neautorizovaného připojení.
54	General	**Fax Receive**	Řídí, zda zařízení smí přijímat příchozí faxové přenosy.	Příjem faxů může vytvářet nekontrolovaný vstupní kanál pro dokumenty a citlivé informace.
55	General	**Command Load and Execute**	Řídí možnost načítat a spouštět příkazy nebo obsah v zařízení.	Možnost načítat a spouštět příkazy zvyšuje riziko provedení neautorizovaného kódu.
56	General	**File System Access Protocols**	Kontroluje protokoly a metody povolené pro přístup k souborovému systému.	Nepotřebné nebo nezabezpečené protokoly mohou zpřístupnit soubory či interní data zařízení.
57	General	**Color Access Control**	Kontroluje omezení a pravidla přístupu k barevnému tisku a kopírování.	Bez omezení může docházet k neoprávněnému využití barevného tisku a obcházení pravidel organizace.
58	General	**Disk Encryption Status**	Ověřuje, zda je interní disk zařízení šifrován.	Při krádeži či vyřazení zařízení mohou být data na disku čitelná bez ochrany.
59	General	**Secure Disk Password**	Kontroluje heslo chránící zabezpečený disk zařízení.	Slabé nebo chybějící heslo snižuje ochranu zabezpečeného disku proti neoprávněnému přístupu.
60	General	**Trusted Platform Module (TPM) Status**	Ověřuje stav Trusted Platform Module (TPM), pokud jej zařízení podporuje.	Neaktivní TPM může snížit ochranu kryptografických klíčů a integrity zařízení.
61	General	**I/O Timeout**	Kontroluje časový limit vstupně-výstupní komunikace zařízení.	Nevhodný timeout může ponechávat otevřené relace nebo způsobovat nestabilní komunikaci.
62	General	**Fax Speed Dial Lock**	Řídí možnost měnit rychlé volby faxu na zařízení.	Neoprávněná změna rychlých voleb může vést k odeslání faxu na podvržené číslo.
63	General	**Cancel Print Jobs**	Řídí oprávnění uživatelů rušit tiskové úlohy.	Příliš široké oprávnění může umožnit uživatelům rušit cizí tiskové úlohy.
64	General	**HP Workpath (HP JetAdvantage)**	Kontroluje stav platformy HP Workpath / HP JetAdvantage pro aplikace v zařízení.	Nepotřebná aplikační platforma rozšiřuje útočnou plochu a počet komponent vyžadujících správu.
65	General	**Information Hiding**	Kontroluje omezení zobrazování citlivých informací na zařízení.	Zobrazené informace mohou prozrazovat uživatele, názvy dokumentů nebo technické detaily zařízení.

Device Discovery | 5 Policy Items

Protokoly používané k vyhledávání a oznamování zařízení v síti.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
66	General	**Service Location Protocol (SLP)**	Kontroluje síťovou službu SLP používanou k automatickému vyhledávání služeb.	SLP může zbytečně zveřejňovat služby zařízení a rozšiřovat síťovou útočnou plochu.
67	General	**IPv4 Multicast**	Kontroluje používání IPv4 multicast komunikace.	Multicast může zpřístupňovat služby širšímu síťovému segmentu a komplikovat omezení komunikace.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
68	General	**Link-Local Multicast Name Resolution Protocol (LLMNR)**	Kontroluje protokol LLMNR pro lokální překlad názvů bez DNS serveru.	LLMNR může být zneužit k podvržení odpovědí a přesměrování komunikace v lokální síti.
69	General	**Web Services Discovery (WS-Discovery)**	Kontroluje WS-Discovery používané k automatickému vyhledávání zařízení v síti.	Automatické vyhledávání může zveřejňovat zařízení a služby v síti i tam, kde to není potřebné.
70	General	**Bonjour**	Kontroluje Bonjour/mDNS službu používanou k automatickému vyhledávání zařízení Apple klienty.	mDNS/Bonjour může propagovat zařízení a jeho služby do lokální sítě bez centrálního řízení.

Printing | 12 Policy Items

Tiskové protokoly a služby, kterými klienti odesílají úlohy na zařízení.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
71	General	**Standard TCP/IP Printing (P9100)**	Kontroluje klasický RAW tisk přes Standard TCP/IP port 9100.	RAW tisk na portu 9100 obvykle neposkytuje šifrování ani silnou autentizaci.
72	General	**AirPrint**	Kontroluje službu AirPrint pro tisk z Apple zařízení bez speciálního ovladače.	AirPrint může umožnit automatické objevení a tisk z klientů mimo standardní firemní tiskový proces.
73	General	**SMB/CIFS Shared Folder**	Kontroluje tisk nebo přístup přes sdílené SMB/CIFS prostředky.	Slabé SMB nastavení může vystavit přihlašovací údaje nebo umožnit přístup k síťovým složkám.
74	General	**Line Printer Daemon/Line Printer Remote (LPD/LPR)**	Kontroluje protokol LPD/LPR pro síťový tisk.	Starší LPD/LPR obvykle neposkytuje moderní šifrování a autentizaci.
75	General	**Internet Print Protocol (IPP)**	Kontroluje nezabezpečenou variantu Internet Printing Protocol (IPP).	Nešifrované IPP může vystavit tisková data a metadata při přenosu.
76	General	**Secure Internet Print Protocol (IPPS)**	Kontroluje zabezpečenou variantu IPP přes TLS/HTTPS (IPPS).	Chybné TLS/certifikátové nastavení IPPS může oslabit ochranu tiskových dat při přenosu.
77	General	**Web Services Print (WS-Print)**	Kontroluje službu WS-Print pro tisk prostřednictvím Web Services.	Nepotřebná služba rozšiřuje síťovou útočnou plochu a možnosti automatického objevení.
78	General	**File Transfer Protocol Client (FTP Client)**	Kontroluje FTP klienta, kterým zařízení navazuje odchozí FTP spojení.	FTP přenáší data a často i přihlašovací údaje bez šifrování.
79	General	**File Transfer Protocol Server (FTP Server)**	Kontroluje FTP server zařízení a možnost příchozího přístupu přes FTP.	Aktivní FTP server může umožnit nešifrovaný příchozí přístup k zařízení.
80	General	**AppleTalk**	Kontroluje podporu historického síťového protokolu AppleTalk.	Historický protokol bez moderních bezpečnostních mechanismů zbytečně rozšiřuje útočnou plochu.
81	General	**Data Link Control (DLC) / Logical Link Control (LLC)**	Kontroluje historické protokoly DLC/LLC používané pro síťovou komunikaci.	Nepotřebné historické protokoly zvětšují počet aktivních komunikačních cest.
82	General	**Novell (IPX/SPX)**	Kontroluje podporu historického protokolu Novell IPX/SPX.	Historický protokol bez současných bezpečnostních mechanismů zbytečně rozšiřuje útočnou plochu.

Digital Services | 11 Policy Items

Digitální odesílání, e-mail, fax, skenování a související workflow.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
83	Fax	**Send Fax**	Řídí, zda lze ze zařízení odesílat fax.	Fax může představovat nekontrolovaný kanál pro odeslání citlivých dokumentů mimo organizaci.
84	Folder	**Send to Folder**	Řídí funkci skenování/odesílání dokumentů do síťové složky.	Chybná oprávnění nebo cílová cesta mohou vést k uložení dokumentů do neoprávněné lokace.
85	E-mail	**E-mail Encryption**	Kontroluje šifrování odchozích e-mailových zpráv z digitálního odesílání.	Bez šifrování mohou být odesílané dokumenty čitelné během přenosu nebo na mezilehlých systémech.
86	E-mail	**E-mail Signing**	Kontroluje digitální podepisování odchozích e-mailů.	Bez podpisu nelze spolehlivě ověřit původ a integritu odeslané zprávy.
87	E-mail	**Send to E-mail (Digital Send)**	Řídí funkci skenování a odesílání dokumentů e-mailem.	Neomezené odesílání e-mailem může vést k úniku dokumentů mimo organizaci.
88	E-mail	**E-mail Alert**	Kontroluje možnost zařízení odesílat e-mailová upozornění.	Nesprávná konfigurace může odesílat provozní informace na nechtěné adresy nebo naopak potlačit důležité alerty.
89	E-mail	**Incoming E-mail (POP3)**	Kontroluje příjem e-mailu prostřednictvím protokolu POP3.	POP3 může přidat nepotřebný vstupní kanál; bez zabezpečení navíc přenáší údaje nešifrovaně.
90	E-mail	**E-mail Domain Restriction**	Omezuje domény, na které lze z digitálního odesílání posílat e-mail.	Bez omezení domén mohou být naskenované dokumenty odesílány na libovolné externí adresy.
91	General	**Job behavior (Automatic Sign Out after Send)**	Kontroluje automatické odhlášení uživatele po dokončení digitálního odeslání.	Po odeslání může zůstat aktivní uživatelská relace a být zneužita další osobou.
92	General	**Allow Access to LDAP Address Book**	Řídí přístup zařízení k LDAP adresáři pro vyhledávání kontaktů.	Neomezený přístup k adresáři může zpřístupnit kontaktní údaje nebo rozšířit možnosti zneužití.
93	General	**Web Scan**	Kontroluje možnost spouštět skenování prostřednictvím webového rozhraní zařízení.	Skenování přes web může umožnit vzdálené získání dokumentu bez fyzické kontroly zařízení.

Network Security | 11 Policy Items

Síťová autentizace, firewall, kryptografické požadavky a ochranné mechanismy.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
94	General	**Internet Protocol Security (IPsec)/Firewall**	Kontroluje, zda je zapnutý a správně nastavený IPsec/firewall zařízení.	Bez filtrování a IPsec může být zařízení dostupné z více sítí a protokolů, než je nezbytné.
95	General	**Internet Protocol Security (IPsec)/Firewall Rule Configuration**	Kontroluje konkrétní pravidla IPsec/firewallu na podporovaných zařízeních.	Chybná pravidla mohou otevřít nechtěné služby nebo zablokovat potřebnou bezpečnou komunikaci.
96	General	**Firewall Rule Configuration (New Gen Devices)**	Kontroluje firewallová pravidla na novější generaci zařízení.	Nesprávná pravidla mohou zvýšit síťovou expozici zařízení nebo obejít segmentaci.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
97	General	**FIPS 140 Compliance Library**	Kontroluje používání kryptografické knihovny v režimu odpovídajícím FIPS 140.	Použití nevyhovující kryptografie může být v rozporu s bezpečnostními nebo regulatorními požadavky.
98	General	**Access Control**	Kontroluje obecná pravidla řízení přístupu k funkcím zařízení.	Příliš volná pravidla mohou umožnit neoprávněné použití funkcí zařízení.
99	General	**Windows**	Kontroluje podporu a nastavení autentizace založené na Windows účtech.	Chybné nastavení Windows autentizace může vést k neoprávněnému přístupu nebo selhání legitimního přihlášení.
100	General	**Verify Certificate for IPP/IPPS Pull Printing**	Kontroluje ověření certifikátu při IPP/IPPS pull print komunikaci.	Bez ověření certifikátu může zařízení komunikovat s podvrženým tiskovým serverem.
101	General	**Enable WINS Port**	Kontroluje, zda je povolen síťový port/služba WINS.	Nepotřebná služba WINS rozšiřuje síťovou útočnou plochu a podporuje zastaralé mechanismy jmenného rozlišení.
102	General	**WINS Registration**	Kontroluje registraci zařízení do služby WINS.	Registrace do WINS zvyšuje závislost na zastaralém mechanismu a může zveřejňovat zařízení v síti.
103	General	**HP Connection Inspector**	Ověřuje stav HP Connection Inspector, který sleduje síťová spojení a hledá podezřelé chování.	Bez aktivní kontroly může podezřelá síťová komunikace zůstat neodhalena.
104	General	**Enable Cross-site Request Forgery (CSRF) Prevention**	Kontroluje ochranu EWS proti útokům Cross-Site Request Forgery (CSRF).	Bez CSRF ochrany může útočník přimět přihlášeného správce k nechtěné změně konfigurace.

Network Services | 20 Policy Items

Webové a vzdálené služby, mechanismy aktualizace firmware a další síťové administrační funkce.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
105	Web	**Web Encryption Settings or Active Ciphers**	Kontroluje povolené verze TLS a kryptografické šifry webového rozhraní.	Slabé TLS verze nebo šifry mohou umožnit odposlech či oslabení zabezpečené webové komunikace.
106	Web	**Require HTTPS Redirect**	Vynucuje přesměrování nezabezpečeného HTTP přístupu na HTTPS.	Povolený HTTP přístup může vést k nešifrovanému přenosu přihlašovacích údajů a konfigurace.
107	Web	**Cross Origin Resource Sharing**	Kontroluje pravidla Cross-Origin Resource Sharing (CORS) pro webové rozhraní.	Příliš volná CORS pravidla mohou zpřístupnit webové rozhraní nedůvěryhodným webovým originům.
108	Web	**Embedded Web Server Access**	Řídí, zda je Embedded Web Server zařízení dostupný.	Zbytečně dostupný EWS rozšiřuje vzdálenou administrační plochu zařízení.
109	Web	**Information Tab**	Řídí dostupnost informační záložky/stránek v Embedded Web Serveru.	Veřejně dostupné informace mohou prozrazovat konfiguraci, sériová čísla nebo síťové údaje.
110	Web	**Phone Home**	Kontroluje funkci Phone Home, kterou zařízení komunikuje s externími službami HP.	Odchozí komunikace k externím službám může být v rozporu s pravidly organizace nebo zvyšovat datovou expozici.
111	Web	**Go Button**	Řídí dostupnost tlačítka Go v Embedded Web Serveru.	Vzdálené ovládání funkce může umožnit neoprávněnou interakci s tiskovými úlohami.
112	Web	**Cancel Button**	Řídí dostupnost tlačítka Cancel v Embedded Web Serveru.	Vzdálené zrušení může umožnit zásah do cizích tiskových úloh.

#	Podoblast	Policy Item	Co kontroluje / k čemu slouží	Typické související riziko
113	Web	**Continue Button**	Řídí dostupnost tlačítka Continue v Embedded Web Serveru.	Vzdálené pokračování může obejít lokální kontrolu operátora nebo uživatele.
114	General	**Novell Remote Configuration (RCFG)**	Kontroluje historickou vzdálenou konfiguraci Novell RCFG.	Historický vzdálený konfigurační protokol může umožnit nechtěnou administrační cestu.
115	General	**Telnet**	Kontroluje službu Telnet pro vzdálenou textovou správu zařízení.	Telnet přenáší přihlašovací údaje i data nešifrovaně a je snadno odposlechnutelný.
116	General	**TFTP Configuration File**	Kontroluje možnost konfigurovat zařízení pomocí TFTP konfiguračního souboru.	TFTP neposkytuje autentizaci ani šifrování a může být zneužit k načtení podvržené konfigurace.
117	General	**HP Jetdirect XML Services**	Kontroluje HP Jetdirect XML Services používané pro síťovou správu a integraci.	Nepotřebné management služby mohou rozšířit vzdálenou útočnou plochu zařízení.
118	General	**Certificate Management Service**	Kontroluje službu správy certifikátů zařízení.	Chybná nebo zbytečně dostupná správa certifikátů může oslabit důvěru a zabezpečenou komunikaci.
119	General	**Legacy Firmware Upgrade**	Kontroluje podporu staršího mechanismu aktualizace firmware.	Starší aktualizační mechanismus může poskytovat slabší kontrolu integrity nebo autentizace firmware.
120	General	**Remote Firmware Upgrade (RFU)**	Kontroluje možnost vzdálené aktualizace firmware (Remote Firmware Upgrade).	Neoprávněná vzdálená aktualizace může změnit firmware zařízení nebo jeho bezpečnostní stav.
121	General	**FTP Firmware Update**	Kontroluje možnost aktualizovat firmware prostřednictvím FTP.	Aktualizace přes FTP používá nešifrovaný protokol a může vystavit aktualizační proces manipulaci.
122	General	**Firmware Downgrade**	Řídí, zda zařízení dovolí návrat na starší verzi firmware.	Návrat na starší firmware může znovu zavést známé zranitelnosti.
123	General	**Device Announcement Agent**	Kontroluje Device Announcement Agent, který oznamuje zařízení službě Instant-On Security.	Automatické oznamování zařízení vytváří další komunikační kanál a musí být řízeno podle politiky organizace.
124	General	**Network Time Server**	Kontroluje konfiguraci síťového časového serveru pro synchronizaci času zařízení.	Nesprávný čas komplikuje auditní logy, certifikáty a korelaci bezpečnostních událostí.

Poznámky k použití

- Policy Item představuje jednotlivé bezpečnostní nebo konfigurační pravidlo, které lze zahrnout do politiky HPSM.
- Ne každé zařízení podporuje všechny uvedené položky. Reálná dostupnost závisí na modelu, firmware a instalovaných funkcích.
- Remediation je dostupná pouze u položek a zařízení, které automatickou změnu podporují a kde ji správce politiky povolí.
- Položky v dokumentu jsou seskupeny podle struktury Policy Editoru HP Security Manager 3.16.

Technický zdroj

HP Security Manager - Policy Editor Settings (Technical White Paper). Pro detailní závislosti, podporované modely a přesné chování jednotlivých nastavení doporučujeme použít aktuální technickou dokumentaci HP.