VARONIS A STANDARDY

Varonis a standardy ISO 27000 PŘEHLED

OBSAH

Varonis a standardy ISO 27000 PŘEHLED

Standardy ISO 27000 zahrnují několik dobře známých a publikovaných standardů spolu s některými vyhrazenými čísly. Všechny společně slouží k zabezpečení informací. Konkrétně ISO 27001 tvoří specifikaci pro řídicí systémy zabezpečení dat (ISMS) a nahrazuje dlouho používané standardy BS7799-2. ISO 27002 pak nahrazuje dobře známé standardy ISO 17799 a naznačuje procesy, které vyhovují standardům ISO 27001. Tento leták popisuje, jak může software firmy Varonis pomoci vyhovět požadavkům standardů ISO.

Mezinárodní organizace pro standardizaci (ISO) je největším světovým producentem standardů. Zastřešuje jednotlivé národní standardy států celého světa, z Ameriky, Evropy i Asie. Standardy jsou vyvíjeny ve spolupráci s odborníky a před publikací podstupují mnoho kontrol a revizí. Standardy ISO 27001 aktualizací a rozšířením standardů BS 7799-2. ISO 27001 „přinášejí model pro ustavení, začlenění, provádění, sledování, udržování a vylepšování systémů pro řízení informací“ (ISMS). ISO 27002 rovněž označují procesy pro zabezpečení informací, avšak rozpracovávají více podrobností pro součásti tvořící ISMS. Zatímco dříve tyto standardy vystupovaly samostatně, nyní ISO 27001 a 27002 tvoří komplexní celek. Jednotliví uživatelé mohou používat jejich kombinaci pro budování ISMS odpovídající velikosti dané organizace a nastaveným pravidlům. Společnosti, které zavedou standardy ISO 27000, tak získají certifikaci pro ISO 27001.

KOMU SLOUŽÍ STANDARDY ISO 27001

Vodítka a certifikační požadavky standardů ISO 2700 jsou určeny všem organizacím, obchodním firmám,orgánům státní správy, akademickým institucím a neziskovým organizacím, které se zajímají o začlenění prostředků pro dlouhodobou ochranu svých informací.
Speciálně ISO 27001 lze využít pro:

- stanovení cílů a požadavků na zabezpečení,
- zajištění efektivní správy zabezpečení,
- dodržení právních předpisů a pravidel,
- zajištění zvláštních požadavků na zabezpečení u konkrétních organizací,
- začlenění nových procesů řízení zabezpečení informací,
- stanovení úrovně dodržování pravidel, nařízení a standardů přijatých danou organizací,
- poskytování relevantních informací o pravidlech zabezpečení, nařízeních, standardech a postupech zákazníkům a obchodním partnerům stejně jako spolupracujícím organizacím,
- zabezpečení informací umožňujících podnikání.

JAK VARONIS APLIKUJE ZÁSADY ISO 27001

Varonis poskytuje komplexní systém řízení ochrany informací pro nestrukturovaná a částečně strukturovaná data – obsah souborových serverů a serverů SharePoint. Přesněji řečeno, řešení Varonis zajišťují, že přístup k datům a použití citlivých a důležitých osobních dat uložených na těchto serverech bude odstupňován a používání citlivých dat bude průběžně sledováno tak, aby organizace mohly přesně a průběžně vyhodnocovat využívání dat jednotlivými uživateli a chování těchto uživatelů.
Varonis vytvořil plně integrovanou skupinu pěti produktů poskytujících komplexní prostředí pro řízení, zabezpečení a hlášení všech aspektů využívání nestrukturovaných a částečně strukturovaných dat. Jde o tyto produkty: DatAdvantage pro Windows, UNIX a SharePoint, Data Classification Framework (DCF) a DataPrivilege.

Varonis DatAdvantage pro Windows, UNIX, a SharePoint

Softwarová řešení Varonis DatAdvantage pro Windows, UNIX a SharePoint shromažďují události uživatelů a přístupu k datům v adresářích na souborových serverech. Sofistikovaná analýza takto shromážděných informací poskytuje podrobný přehled o používání dat a umožňuje stanovení oprávněného přístupu na základě potřeb organizace. Bez potřeby vnitřního přístupu tak Varonis zejména:

- Ochraňuje data doporučeným řízením oprávnění přístupu k datům.
- Omezuje přístup k nestrukturovaným datům na základě potřeb organizace.
- Sleduje a monitoruje každý pokus jednotlivých uživatelů o přístup jednotlivým souborům.
- Přehodnocuje řízení přístupu k obsahu pro jednotlivé účty podle změny jejich charakteru.
- Označuje pravděpodobné vlastníky obchodních dat.

Varonis Data Classification Framework

Varonis Data Classification Framework je instalován jako horní vrstva produktu DatAdvantage a zajišťuje klasifikaci citlivých souborů sledovaného obsahu uložených na serverech SharePoint. Tento nástroj:

- Označuje citlivé soubory na základě nastavených kritérií, řetězců nebo obsahu adresářů.
- Podrobně zkoumá nové a pozměněné soubory.
- Provádí a preferuje prohledávání na základě oprávnění, aktivit, četnosti využití a dalších údajů.
- Označuje oblasti s vysokým rizikem: složky a sítě SharePoint využívané příliš často s ohledem na oprávnění a obsahující závažná citlivá data.

Varonis DataPrivilege

DataPrivilege umožňuje přenášet odpovědnost za řízení označování dat od správců systému k jejich vlastníkům bez narušení infrastruktury nebo přerušení práce. DataPrivilege přináší vlastníkům i uživatelům dat možnost společné komunikace, autorizace a aktivace oprávnění. Varonis DataPrivilege vám umožní začlenit prostředí pro nastavení oprávnění pro data, a zvýšit tak jejich dostupnost za současného omezení rizika. Začleněním nástroje DataPrivilege získáte:

- automatizovaný přehled oprávnění,
- automatizovanou autorizaci,
- ochranu dat omezením chyb v řízení oprávnění,
- řízení přístupu podle potřeb organizace umožněním rozhodování vlastníků dat,
- historii nastavení oprávnění pro zlepšení a zpřesnění nastavení,
- nastavení pravidel pro zvýšení bezpečnosti a soudržnosti.

SEZNAM POŽADAVKŮ PRO VARONIS

V následující tabulce jsou uvedeny jednotlivé rámce ISO 27001. Kde je to vhodné, je uvedeno vysvětlení, jak mohou nástroje Varonis DatAdvantage a DataPrivilege pomoci organizacím vyhovět požadavkům ISO 27001 s ohledem na uložení nestrukturovaných dat na souborových serverech UNIX a Windows nebo na připojených síťových úložištích. Informace uvedené v tabulce popisují pouze malou část toho, co nástroje Varonis dokážou v oblasti správy komplexních nestrukturovaných a částečně strukturovaných dat.

Odstavec	Část	Účel/oblast	
Správa aktiv	**7.1**	Odpovědnost za aktiva	
	7.1.1	Seznam aktiv	Varonis zobrazuje všechny adresáře s obsahem serveru, tok dat k uživatelům a zpět.
	7.1.2	Vlastnictví aktiv	Varonis zobrazuje, kdo je pravděpodobným vlastníkem dat a adresářů.
	7.1.3	Povolené využívání	Varonis sleduje využívání dat na serveru podle uživatelského jména jmen souborů a manipulace a rozpoznává neobvyklé aktivity.
	7.2	Klasifikace	
	7.2.1	Klasifikační vodítka	Varonis umožňuje klasifikaci dat na základě příslušných vodítek a zajišťuje správné použití řízení na základě této klasifikace.
Řízení komunikace a provozu	**10.1**	Provozní postupy a odpovědnost	
	10.1.2	Změna řízení	Varonis sleduje všechny změny systému souborů včetně změn řízení přístupu a bezpečnostních nastavení.
	10.1.3	Rozdělení úkolů	Varonis pomáhá stanovit minimální oprávnění vytvořením seznamu uživatelů, u nichž by mělo dojít k přehodnocení úrovně oprávnění.
	10.2	Řízení služeb třetího řádu	
	10.2.2	Sledování a přehled služeb třetího řádu	Varonis pomáhá sledovat a prověřovat aktivitu služeb třetího řádu pro nestrukturovaná a částečně strukturovaná data.
	10.3	Plánování a přijímání	
	10.3.1	Správa kapacity	Varonis sleduje všechna neaktivní a opuštěná data a jejich velikost pro efektivní využití souborových serverů a síťových úložišť. Nepoužívaná data jsou přesouvána na archivní úložiště.
	10.1	Sledování	
	10.10.1	Záznam kontrol	Varonis poskytuje detailní a vyhledávání umožňující záznamy o kontrolách všech nestrukturovaných a částečně strukturovaných dat na všech úložištích.
	10.10.2	Sledování používání systému	Varonis poskytuje detailní analýzy přístupů k nestrukturovaným souborům ve sledovaných systémech souborů.

Odstavec	Část	Účel/oblast	
Řízení přístupu	11.1	Požadavky na řízení přístupu	
	11.1.1	Pravidla řízení přístupu	Varonis umožňuje vynucení dodržování pravidel přístupu. Vlastníci mohou přijmout nebo odmítnout doporučení pro změny oprávnění.
	11.2.4	Přehled práv uživatelů	Varonis poskytuje prostředky pro hloubkový přehled oprávnění všech uživatelů. Rovněž poskytuje přehled historie oprávnění pro soubory dat, jež vykazují trend příliš liberálního přístupu.
	11.6	Řízení přístupu k aplikacím	
	11.6.1	Omezení práv přístupu	Varonis poskytuje informace o nadbytečném využívání dat, a pomáhá tak dodržovat příslušné požadavky na řízení přístupu.
Správa bezpečnostních informací o událostech	13.1	Hlášení událostí a slabin systému	
	13.1.1	Hlášení o událostech	Varonis hlásí neobvyklé aktivity v přístupu k datům na serverech překračující normální úroveň. Poskytuje automatické výstrahy a podává hlášení o takových aktivitách vlastníkům dat nebo správcům IT.
	13.1.2	Hlášení o slabinách systému	Varonis podává hlášení o datech snižujících úroveň zabezpečení skupin uživatelů nebo nadměrných přístupech, stejně jako o uživatelích a skupinách s příliš častými přístupy.
	13.2	Řízení informací o událostech a vylepšeních	
	13.2.3	Shromažďování údajů	Varonis zaznamenává veškeré aktivity týkající se souborů a umožňuje jejich vyhodnocování.
Shoda	15.1	Shoda s právními požadavky	
	15.1.2	Duševní vlastnictví (IPR)	Varonis pomáhá dodržovat pravidla pro omezení přístupu k chráněným datům. Systém analyzuje vzory přístupů a průběžně doporučuje změny oprávnění přístupů nad nezbytný rámec.
	15.1.3	Ochrana firemních záznamů	Varonis pomáhá chránit citlivé a důležité informace průběžným sledováním přístupu k nim a oprávněným řízením přístupu.
	15.1.4	Ochrana dat a osobních údajů	Oprávnění pracovníci Varonis dostávají pravidelná hlášení o použití dat a přístupu k chráněným údajům, aby bylo zajištěno jejich bezpečné uchovávání.
	15.1.5	Prevence nesprávného používání informací	Varonis významně omezuje nebezpečí ztráty dat jejich nesprávných využíváním díky průběžnému restriktivnímu řízení přístupu podle potřeb organizace.
	15.2	Shoda s bezpečnostními pravidly, standardy a technickými požadavky	
	15.2.1	Shoda s bezpečnostními pravidly	Varonis zajišťuje, že oprávnění mohou nastavovat pouze vlastníci dat a umožňuje auditorům a oprávněným osobám sledovat jednotlivé procesy.
	15.2.2	Kontrola shody s technickými požadavky	Nástroje Varonis umožňují pravidelnou kontrolu dodržování standardů u sledovaných systémů.
	15.3	Kontrola informačních systémů	
	15.3.1	Řízení kontrol systému	Varonis poskytuje detailní přehled všech aspektů používání dat na souborových serverech včetně akcí prováděných správci domény.

VARONIS A ISO 27002

Zatímco ISO 27001 představuje standardy pro správu dat a umožňuje kontrolu a certifikaci organizací, ISO 27002 stanovuje postupy. V následující tabulce jsou uvedeny konkrétní způsoby, jakými produkty Varonis pomáhají organizacím uvádět postupy podle ISO 27002 do praxe.

Odstavec	Část	Účel	
Úkoly správy vlastnictví	6.1	Stanovení vnitřní bezpečnosti	
	6.1.18	Vyhodnocení rizika vznikajícího při nezbytném umožnění přístupu k datům partnerům mimo organizaci.	Produkty Varonis umožňují rychlé rozpoznání nebezpečí týkající se systému souborů a dat SharePoint.
	6.1.19	Zajištění, aby při hodnocení rizika byly posouzeny i důsledky umožnění přístupu k informacím subjektům mimo organizaci.	Varonis pomáhá přesně stanovit úroveň oprávnění pro jednotlivé uživatele a skupiny.
Úkoly správy vlastnictví	7.1	Stanovení odpovědnosti za firemní vlastnictví	
	7.1.1	Ochrana vlastnictví	Produkty Varonis poskytují přehled o tom,kdo k datům přistupuje, a umožňují tak nastavit příslušnou úroveň zabezpečení
	7.1.2	Řízení ochrany vlastnictví	
	7.1.3	Přístup k vlastnictví	
	7.1.4	Určení uživatelů vlastnictví	Produkty Varonis umožňují inteligentní označení a určení vlastníků na základě detailní analýzy aktivit.
	7.1.5	Stanovení odpovědnosti určených uživatelů za ochranu vlastnictví.	
	7.1.6	Stanovení odpovědnosti za udržování řízení zabezpečení vlastnictví.	
	7.1.7	Ustanovení odpovědnosti vlastníků dat za ochranu vlastnictví organizace a umožnění přesunu odpovědnosti na začleněnou správu.	
	7.2	Použití systému klasifikace informací	
	7.2.1	Poskytnutí příslušné úrovně ochrany informací.	Varonis Data Classification Framework rozšiřuje IDU Framework začleněním obsahu klasifikace informací, vytvořeným sledováním souborů a vyhledáváním klíčových slov, frází a vzorců (například pravidelně se opakujících výrazů), které jsou pro organizaci důležité.
	7.2.2	Ustanovení systému klasifikace informací.	
	7.2.3	Využití systému klasifikace pro stanovení úrovní zabezpečení.	
	7.2.4	Určení očekávané úrovně ochrany pro každý stupeň.	
	7.2.5	Stanovení bezpečnostních priorit pro jednotlivé úrovně zabezpečení.	
	7.2.6	Využití klasifikačního systému pro určení informací vyžadujících ochranu na jednotlivých stupních.	
	7.2.7	Využití klasifikačního systému pro určení, které informace budou na jednotlivých stupních zpracovány.	

Odstavec	Část	Účel	
Komunikace a úkoly správy operací	10.4	Ochrana proti škodlivým a pohyblivým hrozbám	
	10.4.4	Detekce pronikání škodlivých programů a nepovolených pohyblivých programů.	Analýza aktivit odhalí možné hrozby a neautorizované procesy.
	10.9	Ochrana elektronických obchodních informací	
	10.9.6	Ochrana dostupnosti informací přístupných z veřejně dostupných systémů.	Viditelnost oprávnění pomáhá zabezpečovat dostupnost informací.
	10.10	Sledování zařízení zpracovávajících informace	
	10.10.1	Sledování systémů zpracovávajících informace pro detekci nepovolených aktivit.	Varonis zaznamenává každou událost týkající se systému souborů, a umožňuje tak provedení podrobné analýzy aktivit. To napomáhá při detekci možných problémů systému, stejně jako ověřování řízení.
	10.10.2	Záznam událostí zabezpečení	
	10.10.3	Využití operačních záznamů pro detekci potíží informačních systémů.	
	10.10.6	Využití sledování systému pro kontrolu efektivity využívání řízení.	
	10.10.7	Využití sledování systému pro ověření, zda zpracování informací odpovídá bezpečnostním pravidlům organizace.	

Odstavec	Část	Účel	
Úkoly správy řízení přístupu k informacím	11.1	Řízení přístupu k informacím	
	11.1.1	Řízení přístupu k firemním informacím.	Produkty Varonis pomáhají zajistit, aby řízení přístupu bylo správně a efektivně nastaveno.
	11.1.2	Ověřování, zda řízení přístupu k informacím nastaveno. vyhovuje firemním požadavkům.	
	11.1.3	Ověřování, zda řízení přístupu k informacím vyhovuje bezpečnostním firemním požadavkům.	
	11.2	Správa uživatelských oprávnění	
	11.2.1	Řízení oprávnění přístupu k informačním systémům.	Varonis pomáhá identifikovat oprávnění pro lepší údržbu vhodných oprávnění pro přístup k informacím
	11.2.2	Ochrana před neautorizovanými přístupy k informačním systémům.	
	11.2.4	Zajištění, že procesy řízení přístupu budou účinné ve všech fázích přístupu uživatele k informacím od přihlášení až po odhlášení.	
	11.2.5	Zajištění, že přístupové procedury budou věnovat pozornost právům přednostního přístupu nadřazeným obvyklému řízení přístupu.	
	11.3	Podpora správných procedur přístupu	
	11.3.1	Zamezení neoprávněného přístupu k informacím a zařízením zpracovávajícím informace.	Varonis pomáhá identifikovat předimenzovaná oprávnění pro lepší údržbu oprávnění přístupu k souborům.
	11.3.2	Ochrana informací a procesů jejich zpracování před nebezpečím jejich ztráty nebo poškození.	
	11.3.3	Ochrana informací a zařízení na jejich zpracování před krádežemi.	Analýza aktivit pomáhá vyhledávat neobvyklé chování uživatelů pro lepší ochranu dat před krádeží.
	11.3.4	Požadavky na pomoc s řízením přístupu k informačním systémům a zařízením na jejich zpracování ze strany oprávněných uživatelů	DataPrivilege automaticky zahrnuje uživatele sdílející oprávnění k přístupu do procesů řízení včetně oprávnění k zobrazení přístupů.
	11.3.5	Stanovení odpovědnosti oprávněných uživatelů pro pomoc s řízením přístupu k informacím a zařízením na jejich zpracování.	
	11.3.6	Upozornění uživatelů na povinnosti spojení s řízením přístupu.	
Úkoly pro rozvoj a údržbu systémů	12.4	Ochrana a řízení systému firemních informací	
	12.4.1	Zajištění zabezpečení systému souborů.	Viditelnost oprávnění, podrobné sledování a klasifikace dat pomáhá chránit systém souborů.
	12.4.2	Řízení přístupu k firemním informacím.	
	12.4.5	Zajištění, že citlivá nebo důležitá data nebudou zahrnuta do testovacího prostředí.	
Úkoly pro správu bezpečnostních událostí	13.1	Hlášení bezpečnostních událostí a slabých míst	
	13.1.1	Zajištění okamžitých hlášení v případě bezpečnostních událostí.	Varonis automaticky podává hlášení vlastníkům dat a správcům IT.

Odstavec	Část	Účel	
Úkoly pro řízení shody	15.1	Shoda s právními požadavky	
	15.1.1	Zajištění, že vaše informační systémy budou odpovídat všem příslušným právním předpisům.	Poskytnutím jistoty v řízení přístupu produkty Varonis umožňují splnit požadavky na shodu v oblasti správy dat včetně PCI, Sarbanes Oxley, HIPAA, Hitech a dalších.
	15.1.2	Zajištění, že vaše informační systémy budou odpovídat všem příslušným bezpečnostním požadavkům.	
	15.1.3	Zajištění, že vaše informační systémy budou odpovídat všem příslušným bezpečnostním požadavkům.	
	15.1.5	Provozování vašich informačních systémů ve shodě s příslušnými pravidly, předpisy a bezpečnostními požadavky.	
	15.1.6	Řízení vašich informačních systémů ve shodě s příslušnými pravidly, předpisy a bezpečnostními požadavky.	
	15.2	Vytváření přehledů o bezpečnostní shodě	
	15.2.1	Zajištění, aby vaše systémy vyhovovaly firemním bezpečnostním pravidlům.	Produkty Varonis poskytují detailní informace o kontrolách aktivity systému souborů a pomáhají organizaci vyhovět bezpečnostním pravidlům.
		Zajištění, aby vaše systémy vyhovovaly firemním bezpečnostním standardům.	
		Přehled zabezpečení firemních informačních systémů.	
		Zajištění pravidelného zpracování přehledů o stavu zabezpečení.	
		Přehled zabezpečení vašich informačních systémů a stanovení, nakolik vyhovují bezpečnostním požadavkům.	
		Kontrola vašich technických zařízení a informačních systémů pro stanovení, nakolik vyhovují stanoveným bezpečnostním pravidlům.	
		Kontrola vašich technických zařízení a informačních systémů pro stanovení, nakolik vyhovují požadavkům na řízení zabezpečení.	
	15.3	Provádění řízených kontrol informačních systémů	
	15.3.1	Provádění kontrol informačních systémů.	Varonis poskytuje detailní informace o kontrolách všech systémů souborů a oprávnění.

O ŘEŠENÍCH VARONIS

Varonis dnes představuje předního inovátora a poskytovatele komplexních akčních řešení pro správu dat. Mezi uživatele těchto řešení patří přední společnosti v oblasti finančnictví, zdravotnictví, energetiky, výroby a technologií po celém světě. Na základě patentovaných technologií a velmi přesných analýz poskytují softwarová řešení Varonis absolutní přehled a kontrolu nad firemními daty a zajišťují, že k těmto datům vždy budou moci přistupovat pouze uživatelé s příslušným oprávněním.

FreeDivision
for safety reasons

FreeDivision s.r.o.
U Pazderek 265/22
181 00 Praha 8 Bohnice
tel: +420 220 972 426
email: info@freedivision.com
www.freedivision.com