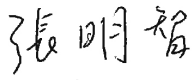
QNAP NAS

Příručka bezpečnosti informací

QNAP SYSTEMS, INC.

Děkujeme, že používáte produkty QNAP a že jste svá data svěřili do úschovy QNAP NAS. Velmi si vážíme vaší podpory a vaši důvěru v nás považujeme za naši nejcennější hodnotu. Za tímto účelem se snažíme o dokonalost neustálým zlepšováním našich produktů a zabezpečení. v dnešním světě s rostoucím počtem útoků, malwaru a bezpečnostních problémů jsme cítili potřebu poskytnout vám následující informace, které vám pomohou aktivně bránit sebe a svůj digitální majetek. Doufáme, že kombinací rad v této příručce a rozumných návyků při používání IT mohou všichni naši uživatelé ochránit svá zařízení a data před současnými i nově vznikajícími hrozbami.

QNAP Systems, Inc.



General Manager

www.qnap.com

Osvědčené postupy pro zlepšení zabezpečení

Metody ochrany dat se neustále snaží držet krok s vývojem hackerských technik. Uživatelé NAS mají k ochraně svých dat a zařízení k dispozici mnoho nástrojů - včetně ochrany heslem, nastavení oprávnění, šifrování na úrovni souborů, aktualizací operačního systému a softwaru, nastavení síťového připojení a aplikací pro zálohování dat a obnovu po havárii. Produkty QNAP mají mnohostranné a robustní funkce zabezpečení informací. Níže je uvedeno devět (9) bodů zabezpečení informací, které našim uživatelům pomohou rychle získat základní znalosti o zabezpečení informací.

1. Odstranění neznámých nebo podezřelých uživatelských účtů

2. Odstranění neznámých nebo zřídka používaných aplikací NAS

3. Zakázat automatické nastavení směrovače v myQNAPcloud

4. Nastavte řízení přístupu k zařízení

5. Nezveřejňujte výchozí číslo portu na internetu

6. Nainstalujte a spusťte nejnovější verzi programu Malware Remover

7. Pravidelně měňte hesla všech uživatelských účtů

8. Aktualizujte nainstalované aplikace na nejnovější verze

9. Zajistěte, aby operační systém a/nebo systémový software vašich síťových zařízení byl vždy aktuální

Později vám postupně vysvětlíme různé návrhy zabezpečení informací společnosti QNAP a dále vytvoříme komplexní plán obrany NAS.

Používejte silná hesla

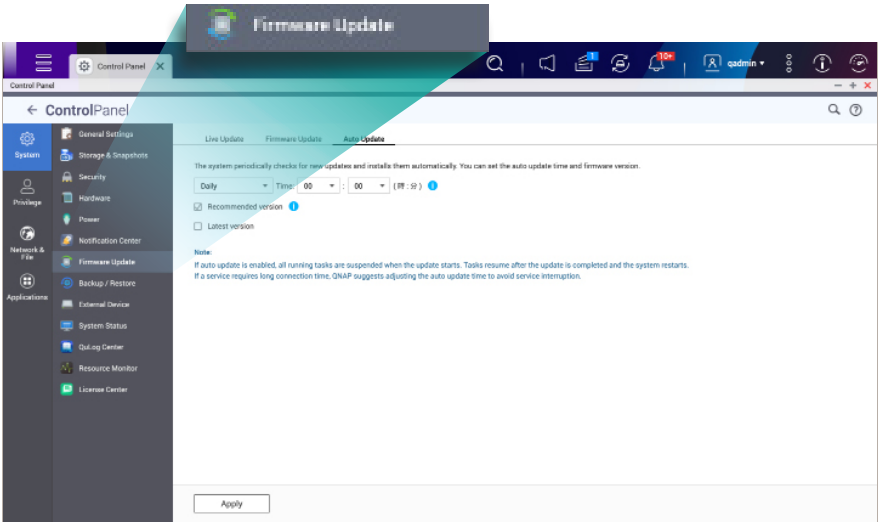
Pokus o přístup k uživatelskému účtu je nejčastějším vektorem útoku hackerů. Obvykle se tak děje tak, že hackeři zkoušejí výchozí nebo běžná hesla nebo využívají sociální inženýrství (například: pokud někdo použil jako heslo jméno domácího mazlíčka nebo dítěte, může ho někdo uhodnout). Chcete-li snížit hrozbu napadení uživatelského účtu, doporučujeme zakázat výchozí účet správce a nařídit všem uživatelům, aby si nastavili silná hesla, jak je popsáno níže.

Podmínka	Popis
Anglická písmena	Použijte směs velkých a malých písmen.
Čísla	Použijte alespoň jedno číslo
Speciální znaky	Použijte alespoň jeden speciální znak (například<?!_* atd.>).
Vyhněte se opakování	Nepoužívejte opakující se znaky (například AAA nebo 111).
Vyloučit jméno uživatele	V hesle nikde nepoužívejte uživatelské jméno, a to ani pozpátku. Například uživatelské jméno je: W user1 a heslo je: 1resu.
Minimální délka	Doporučuje se používat heslo o délce alespoň 8 znaků. Maximální délka hesla je 64 znaků.

Kromě používání silných hesel by uživatelé měli svá hesla také pravidelně měnit. Počet dní platnosti hesla uživatele můžete určit v nastavení systému.

Aktualizace softwaru jsou důležité

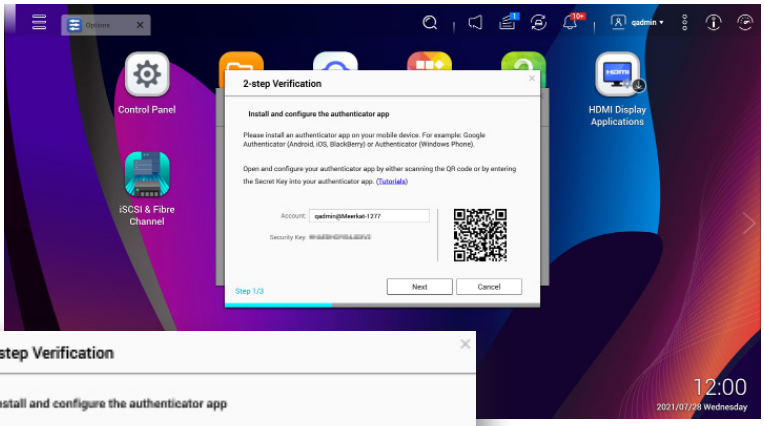
Používání zastaralého softwaru na NAS a dalších síťových zařízeních ohrožuje celou síť. Vývojový tým QNAP aktivně sleduje a opravuje potenciální bezpečnostní chyby, jakmile je objeví, a co nejdříve vydává aktualizace operačního systému a aplikací. Doporučujeme uživatelům, aby své aplikace aktualizovali v Centru aplikací a také aby v části Firmware Update (Aktualizace firmwaru) v systému QTS povolili automatické aktualizace. Webové stránky společnosti QNAP obsahují poznámky k vydání, které poskytují informace o opravách a vylepšeních provedených v nových verzích softwaru.

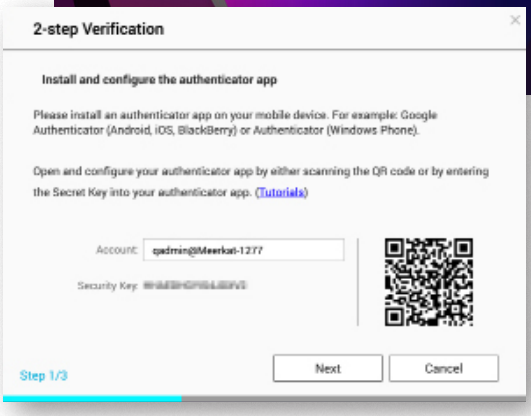


Od verze QTS 4.5.3 bude Centrum aplikací ve výchozím nastavení automaticky aktualizovat aplikace na nové verze (zařízení NAS, která nemohou provést aktualizaci na verzi vyšší než QTS 4.5.3, mohou povolit automatické aktualizace pomocí konzolového rozhraní). Pokud NAS není připojen k internetu, můžete si aktualizace stáhnout z QNAP Download Center a poté je do NAS nainstalovat ručně.

Povolení dvoufázového ověření

Dvoufázové ověření výrazně zvyšuje zabezpečení uživatelských účtů. Pokud je povoleno, budou uživatelé vyzváni k zadání kódu z ověřovací aplikace v mobilním zařízení, než se budou moci dokončit přihlášení ke svému účtu. To přidává uživatelským účtům další vrstvu zabezpečení, která může výrazně snížit možnost neoprávněného přístupu hackerů k uživatelským účtům. Chcete-li použít dvoufázové ověření, musíte si do mobilního zařízení nainstalovat ověřovací aplikaci. Tato aplikace musí k vytvoření ověřovací služby používat algoritmus jednorázového hesla na základě času (TOTP). QTS podporuje aplikace Google Authenticator (Android, iOS a BlackBerry) a Authenticator (Windows Phone) pro dvoufázové ověření.





Pokud dojde ke ztrátě mobilního zařízení s aplikací autentizátoru nebo pokud uživatel nemůže použít mobilní zařízení pro dvoufázové ověření, můžete nastavit alternativní způsob ověření, například zodpovězení bezpečnostních otázek nebo zaslání bezpečnostního kódu e-mailem.

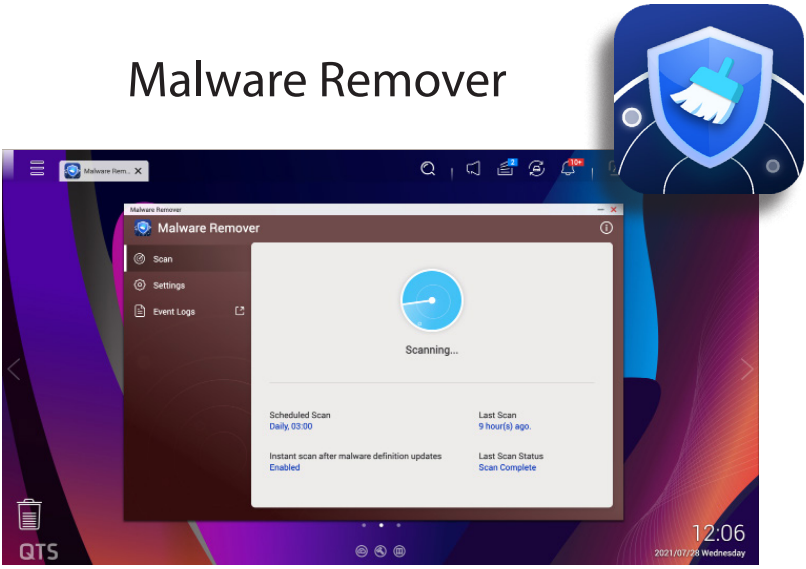
Nechte nás vyhodnotit zabezpečení za vás

Při připojování jakéhokoli zařízení k internetu existují neodmyslitelná bezpečnostní rizika, a proto společnost QNAP poskytla aplikaci Security Counselor. Tato aplikace kontroluje potenciální bezpečnostní zranitelnosti vašeho NAS a poskytuje doporučení pro úpravy konfigurace systému, aby se zabránilo ohrožení vašeho NAS.

V nástroji Security Counselor můžete zadat různé doporučené úrovně zabezpečení na základě požadavků na používání NAS. Kontroly lze provádět také podle plánu. Můžete také upravit další nastavení, včetně blokování IP adres, bezpečnostních pověření a zásad hesel.

Okamžité odstranění hrozeb

Pravidelné skenování může pomoci zjistit, zda byl váš NAS napaden malwarem, a zjištěný malware odstranit. Nástroj Malware Remover také automaticky stahuje nejnovější definice malwaru, aby vám poskytl co nejlepší ochranu před novými a vznikajícími hrozbami malwaru.



Nástroj Malware Remover můžete také nakonfigurovat tak, aby odesílal výsledky skenování do společnosti QNAP, což nám umožní aktualizovat definice malwaru a posílit zabezpečení všech uživatelů QNAP NAS.

Instalace bezpečnostní brány firewall pro NAS

Síťové bezpečnostní hrozby nerozlišují mezi vnitřními a vnějšími sítěmi a síťové firewally (hraniční) nastavené na okraji místních sítí nestačí k zajištění všestranné bezpečnosti. V současné době se do popředí dostává koncept sítí s nulovou důvěrou a vy můžete na zařízení QNAP nainstalovat a povolit bránu QuFirewall a vytvořit tak bránu firewall na bázi hostitele (mikrohranici), která ochrání vaše kritická data a služby.

QuFirewall je bezplatná aplikace QNAP NAS, která umožňuje nastavit pravidla příchozího síťového provozu pro povolení/zamítnutí připojení a zlepšit zabezpečení NAS připojeného k internetu. QuFirewall také podporuje funkci GeoIP, kterou lze použít k detekci a odmítnutí připojení ze zadaných zeměpisných oblastí. Pro ještě lepší ochranu můžete zvážit instalaci populární open source brány firewall pfSense z Virtualization Station Virtual Machine Marketplace.

Nenechávejte svůj NAS vystavený

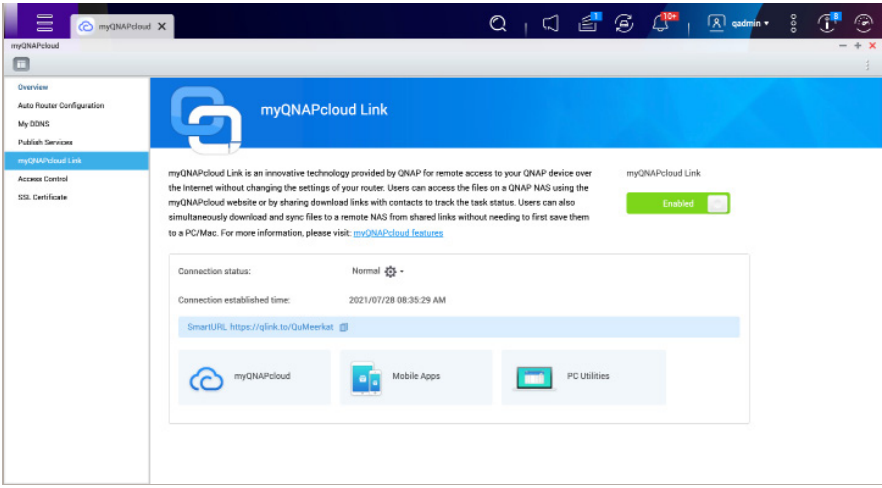
Pokud se váš QNAP NAS připojuje přímo k internetu bez ochrany, je potenciálně zranitelný vůči slídění. Pomocí botnetů nebo webových stránek, jako je Shodan, mohou útočníci potenciálně zablokovat zařízení a zahájit útoky. To se kontroluje v nastavení přesměrování portů směrovačů a modemů. Pokud povolíte ruční přesměrování, automatické přesměrování portů (UPnP; Universal Plug and Play) nebo demilitarizovanou zónu (DMZ), pak je váš QNAP NAS připojen přímo k internetu. K přímému připojení k internetu dochází také tehdy, když QNAP NAS získá veřejnou IP adresu přímo (statická/PPPoE/DHCP).

Pokud potřebujete vzdálený přístup k NAS, je nejbezpečnějším způsobem navázat zabezpečené připojení VPN nebo použít aplikaci myQNAPcloud Link. Pokud tyto způsoby připojení nepoužijete, musíte QNAP NAS nainstalovat za směrovač a bránu firewall. Pokud je NAS umístěn za směrovačem, ale je připojen k internetu prostřednictvím přesměrování portů, měli byste na směrovači zadat nové číslo portu. Nepoužívejte čísla portů jako 22, 443, 80, 8080 nebo 8081.

Bezpečnostní tipy pro vzdálená připojení

Jednou z nejlepších vlastností NAS je univerzální přístup k souborům a službám z jakéhokoli zařízení a kdykoli. Abychom usnadnili vzdálené připojení a zvýšili jeho bezpečnost, vyvinuli jsme aplikaci myQNAPcloud Link, která se připojuje k vašemu NAS (prostřednictvím připojení P2P), takže se můžete bezpečně připojit k NAS, aniž byste potřebovali další nastavení brány firewall nebo přímo odhalili NAS.

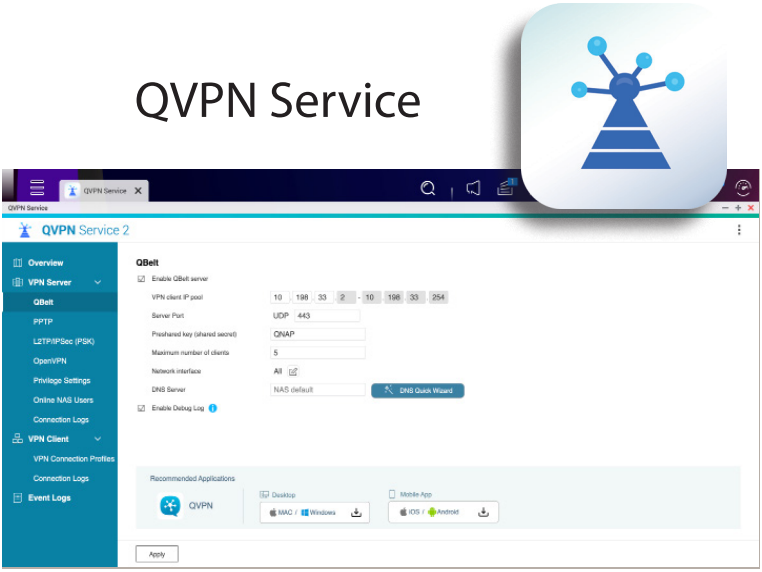
Vzdálené připojení prostřednictvím služeb DDNS dříve vyžadovalo zdlouhavé nastavování, ale myQNAPcloud Link poskytuje jednoduché vzdálené připojení, které vám umožní připojit se k vašemu QNAP NAS, ať jste kdekoli, jako byste ho měli u sebe.



Vytvoření zabezpečeného připojení VPN

Kromě vzdáleného připojení myQNAPcloud Link poskytuje nastavení vlastního serveru virtuální privátní sítě (VPN) na zařízení QNAP NAS pomocí služby QVPN vyšší úroveň zabezpečeného připojení, které umožňuje bezpečnější komunikaci mezi zařízeními a NAS. Kromě toho můžete QNAP NAS připojit i k jiným serverům VPN.

QBelt, exkluzivní protokol VPN QVPN společnosti QNAP, může dále snížit pravděpodobnost odhalení připojení VPN. Počítač nebo mobilní zařízení se může pomocí QVPN Device Client připojit k serveru VPN na QNAP NAS nebo ke službě QuWAN.



Vestavěné bezpečnostní funkce

In addition to the many security-enhancing applications mentioned above, QNAP's NAS operating systems (QTS and QuTS hero) have a wide range of built-in security settings to add extra layers of protection to your NAS.

• Černá a bílá listina IP: Pomocí bílé listiny lze omezit připojení pouze na autorizované IP adresy, zatímco černou listinu lze použít k automatickému blokování připojení určitých IP adres k NAS.

• Automatické blokování: Nastavte NAS tak, aby blokoval uživatele/IP adresy, kteří se po určitém počtu pokusů nepřihlásili. To je užitečné pro zabránění útokům hrubou silou a zajištění bezpečnosti zařízení.

• Připojení HTTPS: Pro zajištění vyššího zabezpečení můžete povolit připojení HTTPS k NAS a zvolit šifrování připojení pomocí certifikátu TLS, který si sami podepíšete/myQNAPcloud/Let's Encrypt.

• Více řešení zálohování: Zálohování: NAS můžete plně zálohovat několika způsoby, včetně snímků a zálohování/synchronizace na vzdálený server nebo do cloudového úložiště.

• Kontrola oprávnění: Kromě kontroly zabezpečení informací poskytuje nastavení oprávnění ke složkám uživatelům větší soukromí, což nejen zajišťuje bezpečnost důvěrných informací, ale také splňuje požadavky právních předpisů.

• Protokoly a oznámení: Systém má zabudované protokoly událostí a oznámení, které zajišťují podrobnou sledovatelnost operací a šetří čas při údržbě IT.

Odstranění neznámých rizik

Uživatelské účty by měly být sledovány a upravovány na základě vašich požadavků. Účty, které již nejsou potřeba, byste měli odstranit nebo zrušit všechna jejich oprávnění, pokud bude účet potřeba později. To můžete provést v nabídce "Ovládací panely" > "Oprávnění" > "Uživatelé". Měli byste také sledovat, jaké aplikace mají uživatelé nainstalované, a ověřit, zda jsou po odebrání uživatelského účtu potřebné. Pokud kdykoli najdete uživatelský účet, který nepoznáte nebo si nepamatujete, že byl vytvořen, měli byste jej okamžitě odstranit.

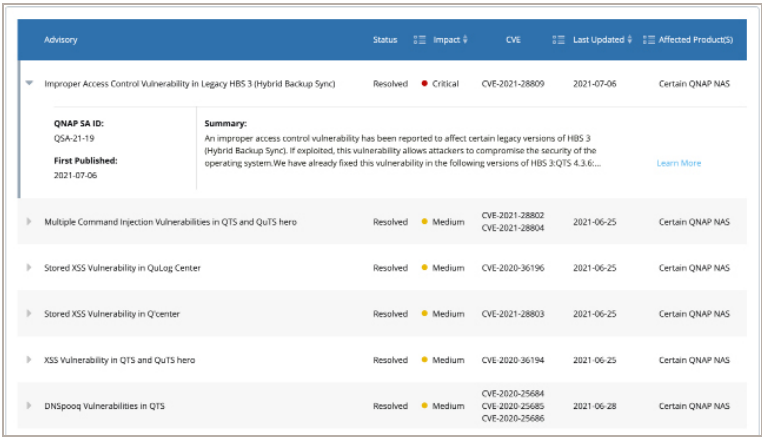
Instalace antivirového softwaru

Kromě bezplatného antiviru ClamAV integrovaného v systému QTS si můžete zakoupit také McAfee Antivirus, známý antivirový software, který poskytuje pokročilou ochranu. Uživatelé QNAP mohou ručně nebo podle plánu skenovat svá data a chránit je před viry, opravovat infikované soubory, dávat infikované soubory do karantény a dostávat nejnovější virové definice na ochranu před novými a vznikajícími viry. Licence McAfee Antivirus lze zakoupit v obchodě QNAP Software Store s platností až na 3 roky.

Bezpečnostní tým společnosti QNAP je v nepřetržité pohotovosti

Společnost QNAP byla v roce 2018 certifikována mezinárodní neziskovou organizací MITRE jako autorita pro číslování CVE. To společnosti QNAP umožňuje přidělovat identifikátory CVE pro bezpečnostní problémy v produktech QNAP. Tým PSIRT (Product Security Incident Response Team) společnosti QNAP přijímá v reálném čase oznámení o zabezpečení informací z celého světa, proaktivně vyšetřuje zranitelnosti, zveřejňuje hrozby a reaguje na oznámení o zranitelnostech do 24 hodin od jejich obdržení.

Doporučujeme uživatelům, aby pravidelně kontrolovali bulletin QNAP Information Security Bulletin a přihlásili se k odběru zpravodaje QNAP Information Security Newsletter, aby získali nejaktuálnější informace a aktualizace. V případě bezpečnostního incidentu dodržujte doporučené postupy týmu QNAP PSIRT, abyste zabránili ohrožení vašeho NAS bezpečnostním incidentem.



Advisory	Status	Impact	CVE	Last Updated	Affected Product(S)
Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync)	Resolved	Critical	CVE-2021-28809	2021-07-06	Certain QNAP NAS
QNAP SA ID: QSA-21-19 **First Published:** 2021-07-06	**Summary:** An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3 (Hybrid Backup Sync). If exploited, this vulnerability allows attackers to compromise the security of the operating system.We have already fixed this vulnerability in the following versions of HBS 3:QTS 4.3.6:...				Learn More
Multiple Command Injection Vulnerabilities in QTS and QuTS hero	Resolved	Medium	CVE-2021-28802 CVE-2021-28804	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in QuLog Center	Resolved	Medium	CVE-2020-36196	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in Q'center	Resolved	Medium	CVE-2021-28803	2021-06-25	Certain QNAP NAS
XSS Vulnerability in QTS and QuTS hero	Resolved	Medium	CVE-2020-36194	2021-06-25	Certain QNAP NAS
DNSpooq Vulnerabilities in QTS	Resolved	Medium	CVE-2020-25684 CVE-2020-25685 CVE-2020-25686	2021-06-28	Certain QNAP NAS

Co mám dělat, když je můj NAS napaden šifrovacím útokem?

Útoky ransomwaru se mohou lišit svými účinky a vektory útoku, takže je obtížné stanovit doporučenou obecnou reakci na útok. Chcete-li se připravit na potenciální útoky, důrazně doporučujeme dodržovat osvědčené postupy pro zálohování a obnovu po havárii: denně zálohovat, ukládat zálohy na více zařízení, používat snímky a snapshoty záloh. Nezapomeňte se také přihlásit k odběru zpravodaje o informační bezpečnosti společnosti QNAP, abyste získali nejnovější aktualizace.

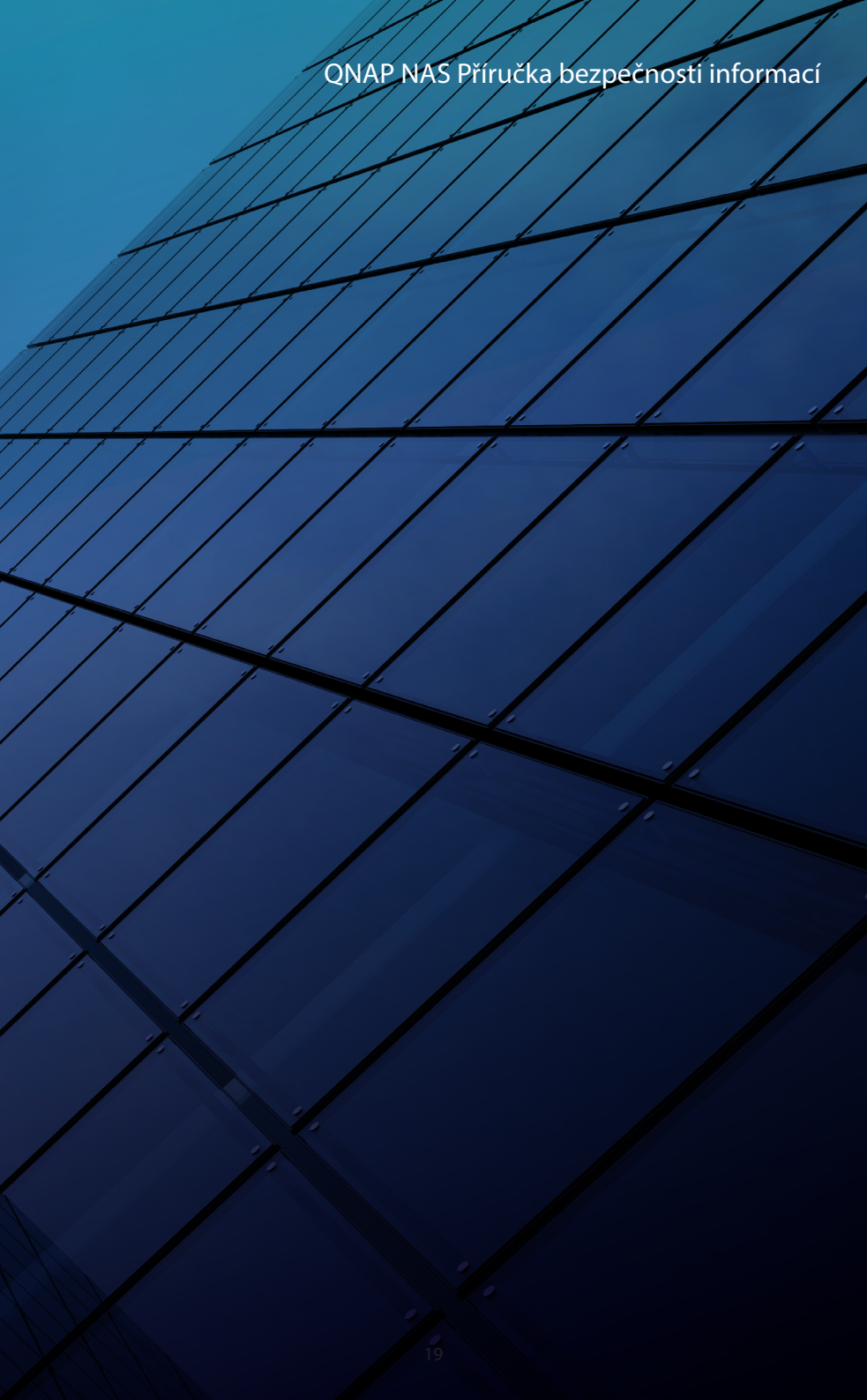
Pokud máte podezření, že byl váš NAS nebo jiné síťové zařízení napadeno (například neobvykle vysoké využití procesoru způsobené neznámými aplikacemi/službami, selhání přihlášení, neznámé soubory ve složkách nebo neoprávněné šifrování souborů), měli byste okamžitě odebrat NAS ze sítě a odpojit síť od internetu. Váš NAS by měl být okamžitě vypnut* a kontaktován Helpdesk QNAP pro další informace. Měli byste také ověřit integritu svých záloh a případně zkontrolovat, zda nebyly kompromitovány.

Aplikaci Malware Remover lze použít k případnému odstranění malwaru ze systému. Ujistěte se, že používáte nejaktuálnější verzi aplikace Malware Remover. Pokud používáte snímky a máte potvrzeno, že soubory snímků nejsou zasaženy, můžete k obnovení cenných dat použít funkci obnovení snímků.

* Ve většině případů je nejlepším postupem okamžité vypnutí NAS při prvním zjištění útoku. Pouze několik šifrovacích útoků může způsobit, že NAS po vypnutí ztratí dešifrovací klíč. Uživatelům doporučujeme věnovat pozornost Informačnímu bezpečnostnímu bulletinu QNAP.

Bezpečnost informací je nejvyšší prioritou společnosti QNAP

Závazek společnosti QNAP v oblasti zabezpečení informací je nekompromisní. Aktivně udržujeme bezpečnost informací a spojujeme síly našich partnerů a komunity, abychom zajistili bezpečnost produktů QNAP pro váš klid.



QNAP SYSTEMS, INC.

TEL : +886-2-2641-2000 FAX: +886-2-2641-0555 Email: qnapsales@qnap.com
Address : 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwan

Netherlands (Warehouse Services)
Email: nlsales@qnap.com
TEL: +31(0)107600830

China
Email: cnsales@qnap.com
TEL: +86-400-028-0079

Japan
Email: jpsales@qnap.com
FAX: 03-6435-9686

US
Email: usasales@qnap.com
TEL: +1-909-595-2782

India
Email: indiasales@qnap.com

France
Email: Frsales@qnap.com

Thailand
Email: thsales@qnap.com
TEL: +66-2-5415988

Germany
Email: desales@qnap.com