Průvodce aplikací

Vodafone Business CyberWall pro Android a iOS

Together we can

vodafone business

Průvodce aplikací Vodafone Business CyberWall pro Android a iOS

Obsah

Android

1. Instalace a aktivace 3
2. Princip ochrany – sledování 3 vektorů 3
3. Hlavní stránka aplikace – status hrozeb dle barev 4
4. Hlavní stránka 4
5. Správa hrozeb 4
6. Nastavení aplikace CyberWall 5
7. Historie 5

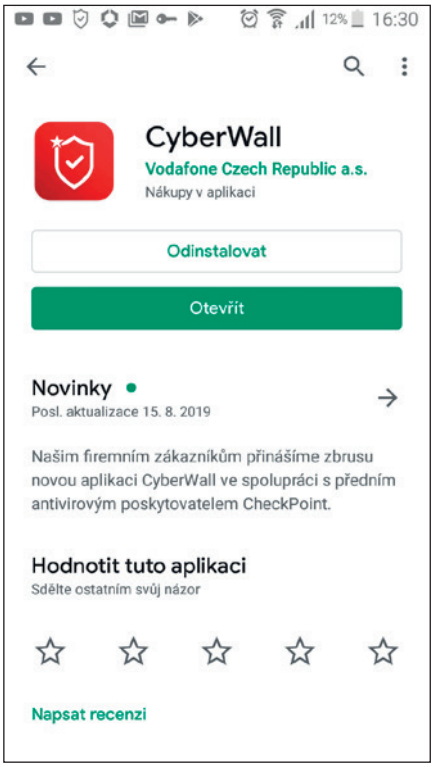
iOS

8. Instalace a aktivace 6
9. SMS phishing – nastavení 6
10. Hlavní stránka aplikace – status hrozeb dle barev 7
11. Nastavení 7
12. Historie 7

Android

Instalace a aktivace

» V zařízení s **OS Android** klikněte na odkaz s licenčním klíčem, který jste obdrželi v SMS hned po aktivaci služby u Vodafonu
» Budete přesměrováni na Google Play store a vyzváni ke stažení aplikace CyberWall
» Po stažení se aplikace automaticky aktivuje, pokud byly splněny předchozí 2 body
» Pokud byla zakoupena licence typu MULTI, tento postup lze opakovat ještě 4× (licence je platná pro 5 zařízení)



Princip ochrany – sledování 3 vektorů

» Bezpečnost zařízení
  › USB debug
  › Neznámé zdroje
  › Zranitelnosti
  › SMS phishing

» Nebezpečné aplikace
  › Instalované aplikace
  › Aplikační soubory uložené v zařízení

» Útoky z internetové sítě
  › Reputace sítě
  › MITM útoky
  › Nešifrované (veřejné) Wi-Fi

Hlavní stránka aplikace – status hrozeb dle barev

	ČERVENÁ	ŽLUTÁ
Aplikace	Škodlivá nainstalovaná aplikace	Škodlivý APK soubor v zařízení
Síť	MITM* útok, nebezpečná síť	Veřejná Wi-Fi
Zařízení	Aktualizace OS	Zranitelnost OS
	Rootovaný device	Nebezpečné nastavení OS

*MITM – Man In The Middle – podstatou tohoto útoku je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem

Hlavní stránka

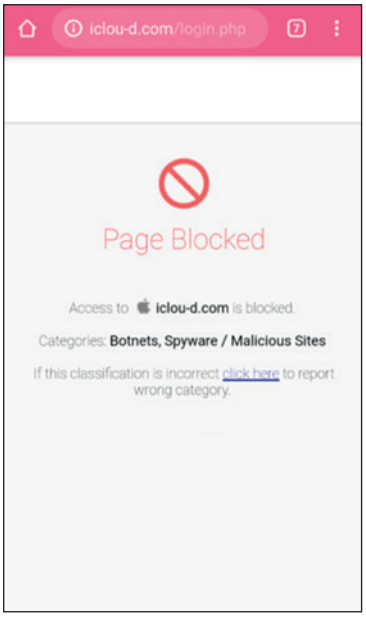
» Celkový status
  › Zobrazuje barvu kruhu podle důležitosti nalezených zranitelností

» Dílčí status pro jednotlivé vektory
  › Zařízení
  › Aplikace
  › Síť

Správa hrozeb

» Hrozba
  › Název
  › Důležitost
  › Popis
  › Doporučení
  › Akce
  › Ignorování

» Prohlížení webu – detekce nebezpečné stránky
  › Blokovaná stránka
  › Adresa stránky (webu)
  › Zablokovaná kategorie

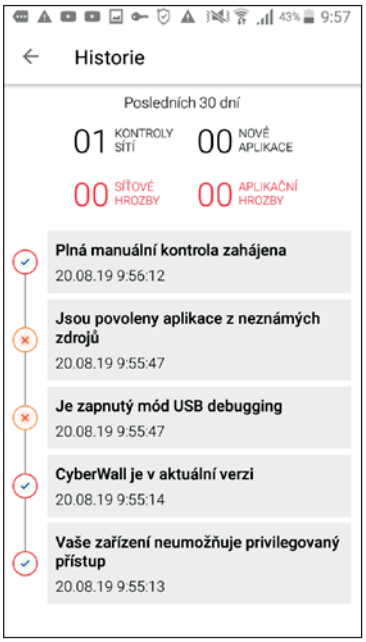


Nastavení aplikace CyberWall

» Bezpečnostní nastavení
  › Notifikace
  › Kontroly na pozadí
  › Přístup k polohovým službám
  › Přístup k úložišti
» Podpora
» Návod

Historie

» Posledních 30 dní
» Kontrola sítí
» Skeny zařízení
» Nové aplikace



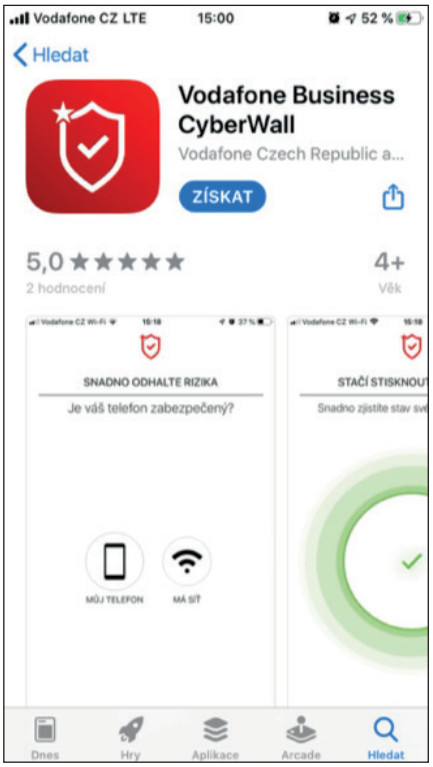
iOS

Instalace a aktivace

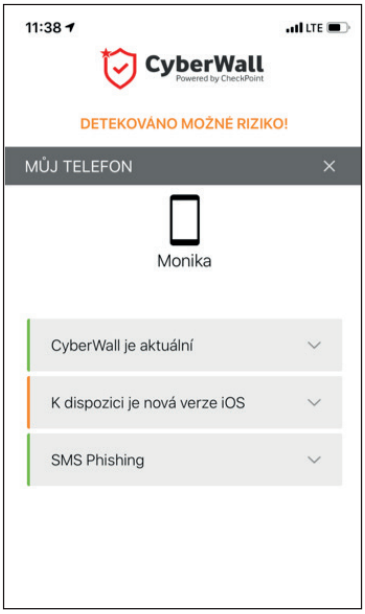
» V zařízení s **iOS** klikněte na odkaz s licenčním klíčem, který jste obdrželi v SMS hned po aktivaci služby u Vodafonu

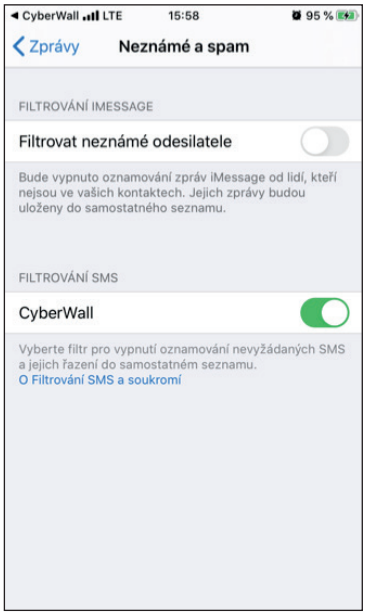
» Po stažení klikněte znovu na odkaz v SMS anebo zadejte licenční klíč z SMS do pole Aktivovat na úvodní stránce aplikace CyberWall

» Pokud byla zakoupena licence typu MULTI, tento postup lze opakovat ještě 4× (licence je platná pro 5 zařízení)



SMS phishing – nastavení





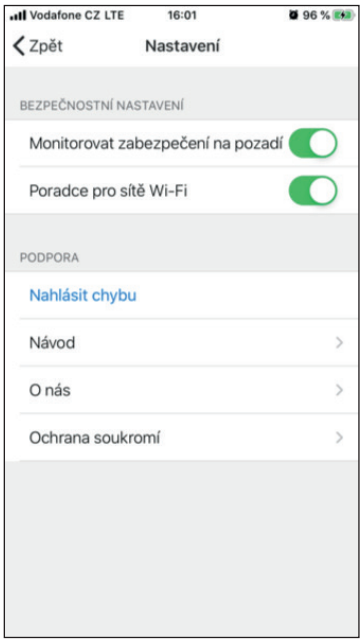
Hlavní stránka aplikace – status hrozeb dle barev

	ČERVENÁ	ŽLUTÁ
Síť	MITM* útok, nebezpečná síť	Veřejná Wi-Fi
Zařízení	Aktualizace OS	Zranitelnost OS

*MITM – Man In The Middle – podstatou tohoto útoku je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem

Nastavení

» **Monitorovat na pozadí** – kontroluje veškeré podezřelé aktivity, nepřetržitě
» **Wi-Fi poradce** – v případě podezřelé sítě doporučí se k ní nepřipojovat
» **Podpora**
» **Historie**



Historie

» Nachází se na hlavní stránce
» Posledních 30 dní
» Kontrola sítí
» Skeny zařízení
» Ověření CyberWall verze

PK8120