Deep Secure information eXchange (iX)

Inline odstranění hrozby z obsahu pro e-mail, přenosy souborů, webové aplikační služby a mnoho dalšího – odstraňuje známé, nově objevené i neznámé hrozby z obchodního obsahu.

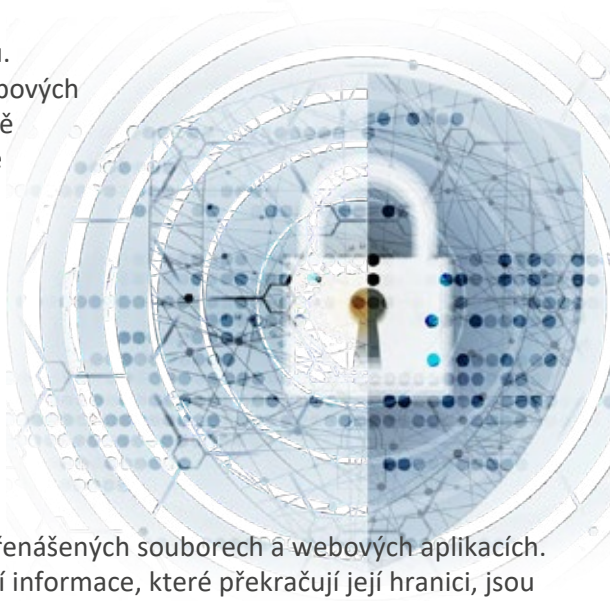
Modul iX od Deep Secure se nasazuje inline na okraj sítě a funguje jako firewall v aplikační vrstvě, který odstraňuje hrozby z obchodního obsahu přenášeného e-mailem, webovými aplikacemi a provozem v síti a protokolech.

Už vás neohrozí ani nově objevené hrozby – zaručeno!

Modul Deep Secure information eXchange (iX) pomocí metody odstranění hrozby z obsahu vždy doručuje bezpečný obsah bez hrozeb, aniž by hrozby potřeboval detekovat nebo izolovat uživatele od obchodního obsahu, který potřebují. Zastavíte ransomware, odrazíte i čerstvě objevené hrozby a odvrátíte steganografické útoky, aniž byste museli obsah podrobně zkoumat nebo se spoléhat na signatury. Ani ty nejpokročilejší cílené útoky a taktika nenápadného ztrácení dat nebudou mít šanci. Díky Deep Secure iX budete zcela chráněni před hrozbou nově vzniklých bezpečnostních útoků skrytých v obchodním obsahu.

Inline odstraňování hrozeb

iX podporuje celou řadu protokolů a souvisejících datových formátů. Umožňuje odstraňovat hrozby z e-mailu, přenášených souborů, webových aplikaci a síťového/protokolového provozu. Umísťuje se na okraj sítě a funguje jako inline komponenta. Z obchodního obsahu odstraňuje hrozby a – v případě webových aplikací – zajišťuje omezení jejich provozu tak, aby odpovídal přednastaveným schématům.



Odstranění hrozeb z obsahu – digitální čistota

Jedinečná technologie transformace obsahu od společnosti Deep Secure předpokládá, že každý obchodní dokument nebo obrázek může obsahovat hrozbu. Na hranici sítě zachycuje obsah a na její druhé straně ho znovu od počátku vytvoří čistý a bezpečný. Tím je hrozba zničena. Od počátku ke konci se nedostane nic než bezpečný obsah. Uživatelé mohou bezpečně a bez narušení pracovat – je zajištěna integrita obchodního obsahu v e-mailech, přenášených souborech a webových aplikacích. A organizace se těší dobré pověsti pramenící z vědomí, že obchodní informace, které překračují její hranici, jsou vždy digitálně čisté a bez hrozeb.

Minimální prostor pro útoky

V případě systémů, které čelí nejpokročilejším útočníkům a vyžadují, aby v nich byl co nejmenší prostor pro útoky, lze nasadit dvojici modulů iX propojených prostřednictvím nástroje High Speed Verifier (HSV) od společnosti Deep Secure. JHSV zajišťuje nezávislé ověřování realizované hardwarovou logikou. Nepoužívá tedy žádný software ani síťové prvky, v nichž by mohla být zneužitelná zadní vrátka nebo kvůli kterým by mohl být zranitelný vůči útokům.

Boj proti steganografickým útokům

Steganografie skrývá data do zdánlivě neškodných souborů. Jde o způsob zakódování tajné zprávy do jiné zprávy, zvané nosič, aby ji mohl přečíst jen její zamýšlený příjemce. Steganografie se už dlouho používá k utajování komunikace před úřady. V poslední době je však na vzestupu takzvaný stegware, tedy využití steganografie kybernetickými útočníky. Pro IT odborníky je to špatnou zprávou, zvláště pro ty, kteří používají nástroje odhalující nebezpečná data. Většinu forem steganografie totiž odhalit nelze. Nástroj iX od Deep Secure ničí stegware ukrytý v obrázcích přenášených e-mailem, zabudovaný ve webových aplikačních službách nebo obsažený v souborech. Tyto vektory tak nelze použít k průniku malwaru, úniku cenných dat ani k provozu ovládacích kanálů (CnC).

Forenzní analýza

Informace pro audit a protokolování lze ukládat externě v datovém skladu organizace a je možno je zasílat systému SIEM.

Hlavní výhody

- Jednoduché nastavení – intuitivní grafické uživatelské rozhraní a konfigurace: nastavení a spuštění za necelých 10 minut.
- Vícekanálové – jeden modul iX může být sdílen více aplikacemi překračujícími hranici.
- Odstranění malwaru – hrozby skryté v dokumentech Office a PDF jsou během transformace odstraněny.
- Odstranění stegwaru – hrozby skryté pomocí steganografie ve webových obrázcích a zdrojích dat ze sociálních sítí (stegware) jsou během transformace odstraněny.
- Dvousměrná ochrana – zabraňuje v průniku malwaru, brání v úniku ukrytých dat a přerušuje kanály CnC.
  Audit a externí protokolování – umožňuje forenzní offline prověření.

Platformy

- Fyzická: Zařízení Deep Secure HRB
- Virtuální: Minimální parametry: 1 procesorové jádro, 4 GB paměti, 50 GB prostoru na pevném disku, 2 síťová rozhraní
- V AWS

Operační systém

- Operační systém Deep Secure (DSOS)

Prohlížeč

- Jakýkoli prohlížeč kompatibilní s HTML5

Podporované typy souborů

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Adobe PDF
- Grafický formát GIF
- Grafický formát PNG
- Grafický formát JPG
- Grafický formát BMP
- Grafický formát TIFF
- JSON
- XML
- CSV
- ZIP
- TXT
- Rozšířená podpora při použit volitelného doplňkového příslušenství

Metody a algoritmus steganografického utajení

- Odhalitelná steganografie
- Neodhalitelná steganografie
- Nahrazení nejméně významného bitu
- Shoda nejméně významného bitu
- Vložení redundantních dat
- Uspořádání palety
- Uspořádání koeficientu F5 DCT

Podporované protokoly

- HTTP/HTTP(S)
- SMTP
- DSFSP (přenos souborů)
- Paketový TCP, UDP

Nasazení

- Uno – jeden modul
- V páru – dva moduly, jeden připojený k nízké síti a druhý k vysoké
- V páru – stejné jako předchozí, moduly však propojuje High Speed Verifier (HSV) od Deep Secure, který omezuje prostor k útoku.

Další informace

Další informace o způsobu nasazení iX v řešeních Content Threat Removal for Mail, Content Threat Removal for File Transfer a Content Threat Removal for Web Services naleznete na adrese **www.deep-secure.com/solutions.**