Ochrona endpoint i systemy DLP

Krajobraz zagrożeń

Współczesne ataki na komputery i urządzenia mobilne przybierają różne formy i rozprzestrzeniają się korzystając z różnych dróg, np.: poprzez zarażone strony WWW, pocztę elektroniczną, zewnętrzne pamięci USB. Pomimo szerokiej dostępności produktów zapewniających bezpieczeństwo, komputery i coraz częściej także smartfony są infekowane w zastraszającym tempie. Tradycyjne metody ochrony nie są w stanie nadążać za gwałtownie zmieniającym się krajobrazem mallware-u. W dobie nowych zagrożeń - kodu polimorficznego (samo -mutującego) oraz APT (Advanced Persistent Threat) tradycyjne systemy antywirusowe nie realizują już swoich "statutowych" zadań. Ochrona endpoint musi reagować na nieznane zagrożenia blokując je zanim wyrządzą szkodę.

Przegląd rozwiązań endpoint security

Systemy ochrony końcówek (endpoint security) realizują funkcje bezpieczeństwa na poziomie komputerów użytkowników oraz urządzeń mobilnych. Podstawowym środkiem ochrony pozostaje nadal system antywirusowy. Obecnie powinien on być traktowany co najwyżej jako uzupełnienie, a nie podstawowy środek bezpieczeństwa. Współczesne systemy endpoint security bazują na trzech mechanizmach ochrony:

- technologia sandbox
- integracja z chmurowymi systemami ochrony
- analiza behawioralna na poziomie działających programów

Mechanizmy te mogą być używane równolegle. Technologia sandbox polega na analizie podejrzanych treści w bezpiecznym środowisku. W praktyce może ona być realizowana na serwerze centralnym lub w chmurze.
Rozwiązania chmurowe (prócz technologii sandbox) funkcjonują także jako wszechstronna, stale aktualizowana baza wiedzy dotycząca mallware-u. Systemy behawioralne na bieżąco

monitorują wykonywany kod poszukując niebezpiecznych zachowań, typowych dla oprogramowania mallware, takich jak np. modyfikacja rejestru połączona z jednoczesnym odwołaniem do nieznanych zewnętrznych serwerów, itp.

Inne funkcje bezpieczeństwa endpoint

- Szyfrowanie dysku wewnętrznego - dzięki niemu bez odpowiedniej autoryzacji nie jest możliwe uzyskanie dostępu do danych, a nawet uruchomienie komputera; funkcja ta jest szczególnie przydatna dla komputerów przenośnych - bardziej narażonych na kradzież lub utratę danych.
- Szyfrowanie nośników zewnętrznych: zapewnia bezpieczne składowanie danych na nośnikach USB i zewnętrznych systemach backupu. Polityka bezpieczeństwa pozwala na zrealizowanie takich ograniczeń jak np. zezwolenie na korzystanie tylko z określonego typu lub egzemplarza nośnika, wymuszenie szyfrowania danych dla określonych typów plików lub aplikacji, itp.
- System VPN - pozwala na realizację bezpiecznego dostępu do zasobów firmowych.
- Ochrona i zarządzanie platformami mobilnymi (smartfony i tablety), czyli oprogramowanie EMM (Enterprise Mobility Management)

stanowi ważny element systemu bezpieczeństwa w środowiskach, w których dopuszczone jest stosowanie własnych urządzeń mobilnych zgodnie z zasadą BYOD (Bring Your Own Device).

Przegląd rozwiązań DLP

Data Leakage Prevention (DLP) - systemy ochrony przed wyciekiem danych zapobiegają niekontrolowanym wypływom danych poprzez: pocztę elektroniczną, nośniki wymienne, portale społecznościowe, komunikatory internetowe, itd. Rozwiązania DLP zapobiegają zarówno intencjonalnej kradzieży cennych danych jak i ich utracie spowodowanej przez zaniedbania, błędne procedury lub wadliwie działające oprogramowanie. DLP może też być ważnym elementem zapewniającym spełnienie określonych norm i wymagań zarówno branżowych (np. bankowych) jak i uniwersalnych, np. dyrektywy GDPR. Kluczową funkcją systemu DLP jest umiejętność identyfikacji wrażliwych danych - mogą być one rozpoznane na podstawie lokalizacji, autora, a także zawartości - np. dokumenty zawierajace numery kont bankowych.

Zarządzanie i monitoring

Ważną funkcją współczesnych systemów ochrony endpoint i DLP jest możlwość centralnego zarządzania oraz monitoringu. Wiedza o aktualnych zagrożeniach staje się równie ważna jak ochrona przed nimi. Dlatego też centralna konsola jest kluczowym elementem zarówno systemu endpoint protection jak i DLP.

CC oferuje

W dziedzinie opisywanych rozwiązań ochrony endpoint oferujemy nie tylko dostawy oprogramowania ale także pełną gamę usług: prowadzimy analizę potrzeb klientów, projektujemy systemy bezpieczeństwa oraz integrujemy je z systemami zdalnego dostępu, infrastrukturą VPN, systemem domenowym, itd. Realizujemy testy oraz diagnostykę istniejącej infrastruktury, wykonujemy częściowe lub pełne migracje rozwiązań sieciowych, prowadzimy nadzór oraz utrzymanie w trybie 24x7, a także realizujemy szkolenia warsztatowe. Wszystkie usługi wykonywane są przez naszych pracowników posiadających certyfikaty inżynierów danego producenta - posiadamy i utrzymujemy aktualne certyfikacje wszystkich kluczowych, wymienionych niżej dostawców rozwiązań sieciowych.

DLP i klasyfikacja dokumentów

Ważnym uzupełnieniem systemu DLP jest oprogramowanie klasyfikujące dokumenty - pozwala ono na przypisywanie tworzonym dokumentom określonego poziomu poufności, a następnie kontrolę obiegu takich dokumentów niezależnie od tego, czy są kopiowane częściowo lub w całości jako pliki, wysyłane poczta elektroniczną, przekazywane do aplikacji Web, itd.

Producenci:
Boldon James, Check Point, CoSoSys, Forcepoint, Palo Alto Networks, Sophos, TrendMicro

CC
Otwarte Systemy
Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail: sales@cc.com.pl

Więcej informacji znajdziecie Państwo w Internecie, na stronach:
http://www.cc.com.pl/

Kontakt:
Kontakt ogólny: cc@cc.com.pl
Dział Handlowy: sales@cc.com.pl
Dział Techniczny: tech@cc.com.pl