Prinect

Poradnik
Ransomware. Jak się bronić?

HEIDELBERG

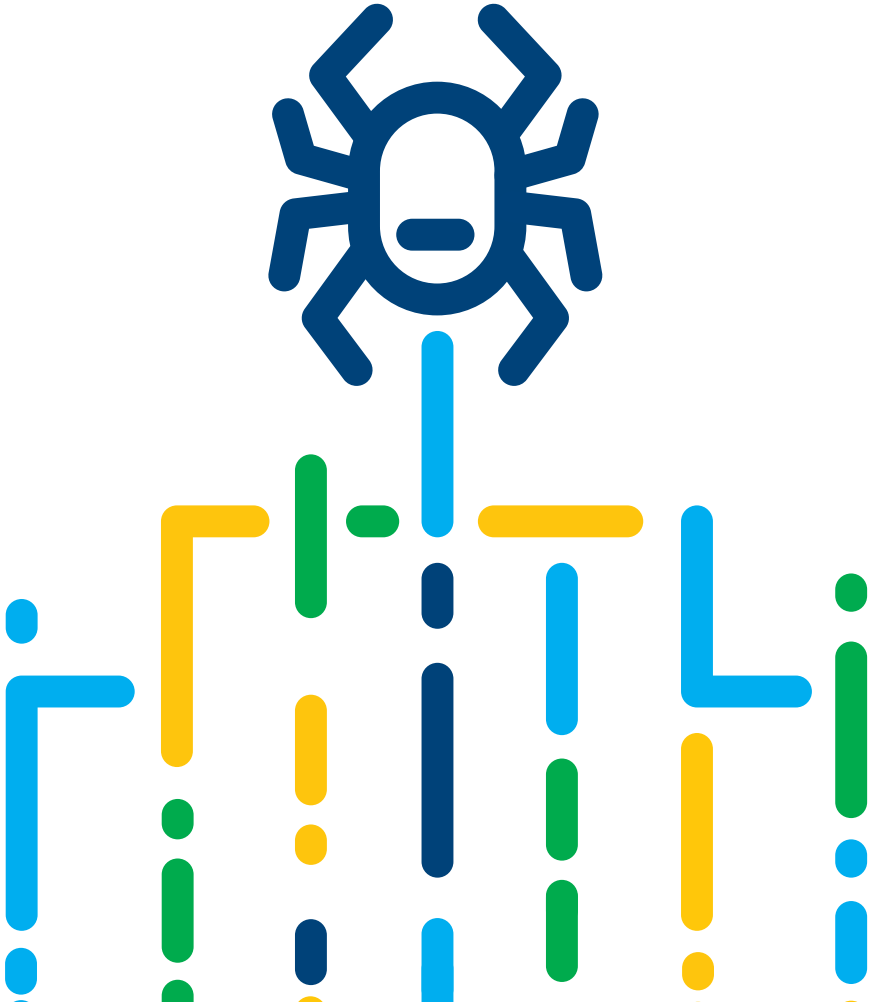
Nie wystawiaj drukarni na ryzyko. Ransomware to poważny problem.

Ransomware* jest potencjalnie bardzo poważnym problemem. Może to być kosztowne doświadczenie i może wpłynąć na reputację Twojej firmy. Bez względu na to czy jest to duża, czy mała firma. Ataki związane z bezpieczeństwem nasilają się, a ofiary doświadczają poważnych zakłóceń związanych m.in. z produkcją.

Broniąc się przed Ransomware, masz **ograniczony wybór:**

- Zainwestuj czas i pieniądze, aby zapobiec niebezpieczeństwu.
- Zainwestuj czas i pieniądze, aby zmniejszyć szkody po ataku przez Ransomware (następnie inwestując czas i pieniądze w zapobieganiu na przyszłość).
- Możesz mieć nadzieję, że nic złego się nie przydarzy.

**Ransomware* (inne określenie: oprogramowanie szantażujące; ang. ransomware – zbitka słów ransom „okup" i software „oprogramowanie") – typ szkodliwego oprogramowania z dziedziny kryptowirologii, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego; Wikipedia [dostęp 2020.02.26]*



Spis treści

Jak się obronić przed Ransomware?
9 kroków, które należy wykonać:

1 Zainstaluj najnowsze oprogramowanie
Upewnij się, że stosujesz najnowsze aktualizacje programowania. Zwłaszcza dotyczy to aktualizacji oprogramowania związanego z bezpieczeństwem:

a. Microsoft Windows Operating System: aktualizacje na serwerach i stacjach roboczych oraz aktualizacje oprogramowania Firmware i BIOS,
b. MacOS – aktualizacje na komputerach Apple.
c. Aktualizacje oprogramowania w całej infrastrukturze. Rozwiązania takie jak firewall i odpowiedni osprzęt sieciowy, a także aplikacje, w szczególności przeglądarki internetowe.

UWAGA: Aktualizacje to nie nowsze wersje.
Aktualizacje to zmiany dla danej wersji systemu operacyjnego, podczas gdy nowsze wersje migrują Cię do nowej wersji systemu operacyjnego z nowymi funkcjami. Instaluj nowe wersje systemu operacyjnego, tylko gdy są obsługiwane przez Heidelberg Prinect oraz inne aplikacje, których używasz.

2 Zainstaluj oprogramowanie antywirusowe
Wdroż oprogramowanie antywirusowe na wszystkich serwerach i stacjach roboczych. Wdrażanie tylko na kilku stworzy ryzyko, że Ransomware dostanie się i przejdzie na inny. Oprogramowanie antywirusowe może spowolnić działanie systemu, w tym oprogramowania Prinect. Heidelberg nie zaleca żadnego produktu antywirusowego ani dostawcy i nie ma wskazówek dotyczących konfigurowania ustawień bezpieczeństwa / wydajności ponieważ różnią się one w zależności od produktu.

3 Stosuj „dobre praktyki”
Postępuj zgodnie z zaleceniami dostawcy i branżowymi „najlepszymi praktykami” chroniącymi Twój sprzęt. Istnieją różne standardy bezpieczeństwa, np. PCI-DSS lub HIPPA.

4 Zawsze rób kopie zapasowe
Wykonuj regularnie kopię zapasową systemów.

5 Wdróż domenę
Jeśli nie jesteś jeszcze w domenie, zastanów się nad wdrożeniem takiej, w której można administrować zasadami bezpieczeństwa z centralnej lokalizacji.

6 Stosuj zasady i procedury
Ustal zasady i procedury, aby zmninimalizować ryzyko udanego ataku.

a. Użytkownicy powinni unikać dostępu do osobistej poczty e-mail z komputerów służbowych.
b. Użytkownicy powinni unikać instalowania niechcianego oprogramowania na komputerach służbowych.
c. Użytkownicy powinni unikać dostępu do swoich mediów społecznościowych z komputerów służbowych.
d. Użytkownicy nie powinni klikać łączy w wiadomościach e-mail od nieznanych lub podejrzanych nadawców.
e. Należy wymagać aby użytkownicy stosowali silne hasła.

7 Używaj tylko markowego oprogramowania
Poza tym, że jest bardziej dopracowane i działa stabilniej, zazwyczaj jest bardziej niezawodne od strony bezpieczeństwa.

8 Eliminuj przestarzały sprzęt i oprogramowanie
Eliminuj sprzęt i oprogramowanie dla którego nie ma wsparcia technicznego lub jest ono niewielkie. Np. jeśli nadal używasz systemu Microsoft Windows Server 2003, dla którego Microsoft zakończył wsparcie kilka lat temu. Gdy nie ma wsparcia, nie ma nowych aktualizacji zabezpieczeń.

9 Chroń swój system produkcyjny Heidelberg Prinect

a. Aktualizuj oprogramowanie Prinect Workflow za pomocą Prinect Maintenance Center.
b. Upewnij się, że użytkownicy logują się przy użyciu własnego konta użytkownika i ustawień logowania do systemu operacyjnego.
c. Nie dawaj każdemu użytkownikowi uprawnień administratora do systemów produkcyjnych.
d. Nie używaj użytkownika „Prinect” do normalnej produkcji i upewnij się, że zmieniłeś domyślne hasła.
e. Zaostrz zasady udostępniania zasobów w systemie. Pełnych praw dostępu nie muszą mieć wszyscy. Heidelberg Prinect Production Manager nie korzysta z ukrytych zasad udostępniania (Hidden Administrative Shares), ale warto sprawdzić czy nie używa ich jakiś inny program, (narzędzia do zarządzania IT).
f. Korzystaj z Prinect Security Tool w Cockpit Administration.

PAMIĘTAJ: Heidelberg nie ma możliwości wyegzekwowania powyższych zasad, a nasi klienci różnią się pod względem wielkości i potrzeb w zakresie bezpieczeństwa, ale im więcej możesz zrobić, aby zająć się kwestią bezpieczeństwa, tym lepiej.

Jak sprawdzić czy mamy Ransomware?
Objawy są następujące:

Pliki się nie otwierają
Nagle nie można otworzyć plików i pojawiają się błędy mówiące, że „plik jest uszkodzony" lub „ma niewłaściwe rozszerzenie".

Dziwne nazwy plików
W katalogach znajdują się pliki o nazwach takich jak „HOW TO DECRYPT_INSTRUCTIONS.HTML".

Nie można zamknąć okien
Zostało otwarte okno przez aplikację Ransomware, którego nie można zamknąć.

Instrukcje dotyczące zapłaty za pliki
Na pulpicie pojawiają się instrukcje w jaki sposób trzeba zapłacić, aby odblokować swoje pliki.

Ostrzeżenie o odliczaniu
Program ostrzega, że trwa odliczanie, a okup wzrasta i nie będzie można odszyfrować plików.

Jak Ransomware do nas dotarło?
Najczęstsze drogi infekcji:

Otwieranie podejrzanych wiadomości e-mail
Jeśli otrzymasz wiadomość e-mail z załącznikiem lub linkiem, aby pobrać oprogramowanie, otwierając załącznik lub klikając w link bez weryfikacji jego autentyczności, możesz zainfekować się Ransomware. **Jest to zdecydowanie najczęstszy sposób infekcji.**

Pobieranie niezweryfikowanych plików
Infekcje Ransomware mogą również wystąpić poprzez pobieranie plików z zainfekowanej witryny za pomocą starej przeglądarki internetowej (lub wtyczki / dodatku). Zaatakowana witryna uruchamia tak zwany „zestaw exploitów", który sprawdza luki w zabezpieczeniach, takie jak systemy operacyjne bez aktualizacji.

Hakerzy
Innym sposobem infekcji przez Ransomware jest haker oferujący darmowe oprogramowanie. Dotyczy to często nielegalych wersji drogich gier lub programów, darmowych gier lub ich modyfikacji, treści dla dorosłych, wygaszaczy ekranu, kodów do gier online lub „obejść" za płacenie za dostęp do strony internetowej. W ten sposób haker może ominąć dowolną zaporę lub ustawienia poczty. Podczas instalacji oprogramowania instaluje się również Ransomware, który uaktywnia się po kilku dniach, tygodniach, a nawet miesiącach.

Remote Desktop Protocol (RDP)
Protokół RDP (Remote Desktop Protocol) służy do zdalnego logowania na komputerach z systemem Windows i pozwala użytkownikowi kontrolować ten komputer tak, jakby przed nim siedział. Protokół RDP zazwyczaj używa do komunikaji portu 3389, a jeśli Twoja firma zezwala na tego rodzaju ruch z Internetu przez zaporę, hakerzy mogą wykorzystać narażone komputery do rozprzestrzeniania Ransomware w Twojej sieci.

Co zrobić, gdy zaatakuje Ransomware?

4 kroki, które należy wykonać:

1 Natychmiast odłącz się od sieci

Jak najszybciej odłącz każdy zainfekowany komputer od sieci. Odłącz każdy kabel Ethernet, wyłącz wszelkie funkcje bezprzewodowe, takie jak Wi-Fi lub Bluetooth, i odłącz urządzenia pamięci masowej.

Zanotuj informacje dotyczące zainfekowanego komputera:

- Mapowane/dzielone foldery z innych komputerów
- Pamięci USB
- Zasoby w chmurze, takie jak Microsoft OneDrive, Google Drive, DropBox itp.

2 Sprawdź swoje komputery

Zinwentaryzuj wszystkie komputery i sprawdź, czy nie mają oznak szyfrowania.

3 Dowiedz się:

- Jaki Ransomware Cię zaatakował
- Czy inne komputery w sieci zostały zarażone
- Który komputer był pierwszy zainfekowany, tzw. „Pacjent Zero". To punkt wejścia. Zazwyczaj robi się to sprawdzając, kto jest właścicielem zaszyfrowanych plików. Aby zaszyfrować plik, Ransomware musi otworzyć się i zapisać w pliku, co oznacza, że własność pliku ulegnie zmianie u użytkownika, który został zainfekowany.

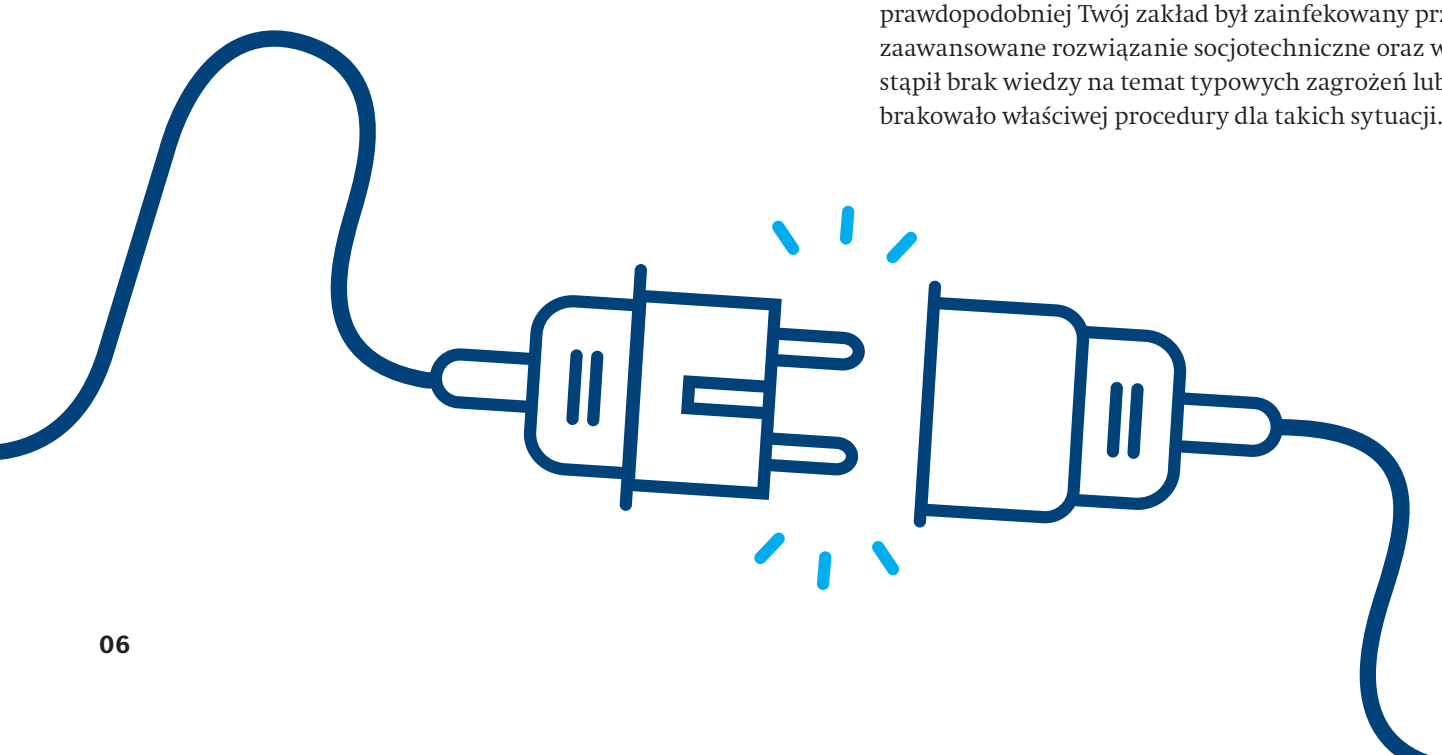
4 Zdecyduj, którą z trzech dróg wybrać:

- **OPCJA 1:** Załaduj ponownie system i zainstaluj oprogramowanie. Oznacza to albo rozpoczęcie od nowa, albo, jeśli masz dobrą kopię zapasową, przywrócenie danych i konfiguracji. Oczywiście jeśli masz ostatnią kopię zapasową, wiadomo, że jest dobra i masz pewność, że wyeliminowałeś wirusa Ransomware z zakładu.

- **OPCJA 2:** Istnieje kilka narzędzi służących do usuwania oprogramowania Ransomware. Heidelberg nie popiera takich narzędzi, ale na pewno możesz je wypróbować, szczególnie jeśli nie masz dobrej bieżącej kopii zapasowej Twojego systemu. Musisz zdecydować, czy czujesz się z nimi komfortowo, czy bardziej sensowne jest zatrudnienie profesjonalisty. To może, ale nie musi, zadziałać.

- **OPCJA 3:** Zapłać okup – zakładając, że masz lub wiesz, jak zdobyć Bitcoiny, które (najprawdopodobniej) będą wymaganą formą płatności i że masz przeglądarkę TOR. Hakerzy często przekierowują Cię na stronę hostowaną w sieci TOR. Płacenie okupu nie gwarantuje, że wszystko wróci do normy lub nie zostaniesz ponownie zainfekowany. Jest to opcja, której prawdopodobnie chcesz uniknąć, jeśli to w ogóle możliwe.

Na przyszłość: Należy wdrożyć profilaktykę dla całego zakładu. Musi to obejmować szkolenie w zakresie Świadomości Zagrożeń dla użytkowników, ponieważ najprawdopodobniej Twój zakład był zainfekowany przez zaawansowane rozwiązanie socjotechniczne oraz wystąpił brak wiedzy na temat typowych zagrożeń lub brakowało właściwej procedury dla takich sytuacji.



Co może zrobić Heidelberg, jeśli dotknie mnie Ransomware?

Niestety po infekcji Ransomware firma Heidelberg niewiele może zrobić. Najpierw musisz usunąć wirusa, a następnie ponownie uruchomić system(y) i zainstalować ponownie oprogramowanie.
Uwaga: odzyskiwanie systemu po ataku wirusów nie jest objęte umową serwisową ani gwarancją, a usługi te są rozliczane według obowiązujących stawek.

Co jeszcze mogę zrobić, aby chronić swój zakład?

Możesz rozważyć włączenie ubezpieczenia od ryzyk cybernetycznych do zakładowego programu zarządzania ryzykiem. Pamiętaj, że trzeba spełnić pewne wymagania. Na przykład może być konieczne określenie Inspektora Ochrony Danych (IOD), utworzenie Zespołu Reagowania na Incydenty i wdrożenie sprawdzonego planu ochrony. Ponadto prawie wszystkie polisy dotyczące cyberbezpieczeństwa będą wymagały terminowego zgłaszania naruszeń.
Co zaskakujące, taka polisa prawdopodobnie ma większy sens w przypadku mniejszych drukarń, które nie mają dedykowanego personelu IT dbającego o bezpieczeństwo.

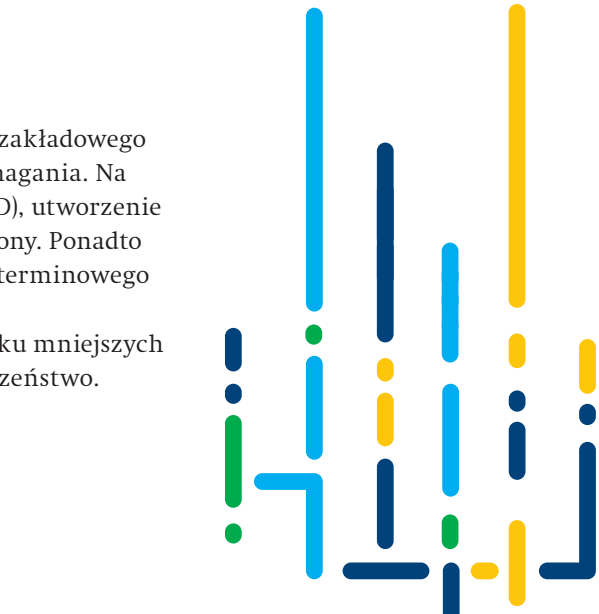
Podsumowanie

Mamy nadzieję, że nigdy nie będziecie Państwo mieć do czynienia z Ransomware. Odzyskanie zajmuje średnio 3 dni i kosztuje dziesiątki tysięcy złotych. Ransomware to problem, który lepiej rozwiązywać wcześniej niż później – naprawdę obowiązuje stare powiedzenie „Lepiej zapobiegać niż leczyć". Należy sprawdzić bezpieczeństwo drukarni i uwzględnić je w budżecie, aby wyeliminować wszelkie luki w ochronie. Heidelberg posiadając wiedzę w tym zakresie może udzielić porady i wskazówek.

Koniecznie:

- Ustal politykę dopuszczalnego użytkowania
- Wzmocnij infrastrukturę IT zakładu
- Wzmocnij ochronę przekierowań sieciowych
- Wzmocnij swój serwer Prinect

Zapytania prosimy kierować do Zastępcy Dyr. Serwisu, Zbigniewa Kosior vel Kosiorka:
tel. 22 5789 260, zbigniew.kosiorek@heidelberg.com



Heidelberg Polska Sp. z o.o.
ul. Popularna 82
02-226 Warszawa
info.pl@heidelberg.com
tel. 22 57 89 000
www.heidelberg.com/pl

Redakcja
Opracowanie graficzne, teksty: Heidelberg USA
Tłumaczenie, opracowanie wersji polskiej,
uzup.: Heidelberg Polska
Wydanie: 03/2020

8480