Jeśli dojdzie do utraty danych, musisz przygotować procedurę poinformowania GIODO, ale także i klientów. Przyda ci się na pewno pomoc prawnika. Warto już wcześniej zdobyć kontakt do kancelarii, która wspiera firmy w takich sprawach, bo tu każda godzina ma znaczenie.

Jeśli spotkasz się z atakiem typu ransomware, czyli zablokowania komputerów, musisz szybko podjąć decyzję – płacisz czy nie. Gdy masz zabezpieczone dane i tracąc dostęp do jednego komputera, problem nie jest duży. Jeśli jednak tracisz dostęp do całego sprzętu w firmie... Na rynku są eksperci, którzy zajmują się takimi tematami, również z nimi warto wcześniej się skontaktować i zdobyć informacje o ich działaniach. Na rynku dostępne są także ubezpieczenia od cyberataków. Często w ramach tego typu produktów mamy możliwość skorzystania z pomocy technicznej.

I nie zapomnij o posiadaniu tych kontaktów nie tylko w formie cyfrowej, ale także papierowej. Bo jeśli stracisz też dostęp do swojego komputera, na nic ci się nie zdadzą.

PO PIĄTE, UCZ SIĘ NA BŁĘDACH INNYCH

Historie wielu porażek związanych z cyberbezpieczeństwem są jawne. Można na ich przykładzie nauczyć się, jakich błędów unikać i z czym możemy się mierzyć. Weźmy wydarzenia ostatnich miesięcy – hakerzy z grupy Anonymous wypowiedzieli wojnę Rosji w związku z wojną w Ukrainie i dokonali szeregu ataków typu DDOS na strony rządowe i banków. W efekcie wiele instytucji i firm straciło dostęp do swoich stron internetowych. Taki atak może także dotknąć twoją firmę. Czy wiesz, co wtedy zrobić?

Sprawdź historie m.in. wycieku danych z Morele.net. Na firmę została nałożona kara prawie 3 mln zł za utratę danych klientów. W Polsce regularnie wyciekają także dane studentów różnych uniwersytetów. Ciekawy przykład stanowi również niedawny wyciek danych o sprzęcie wykorzystywanym w Wojsku Polskim. Wszystko to przez próbę ułatwienia sobie życia przez jednego z programistów, który popełnił przy tym błąd.

Mając takie doświadczenia, wdróż stosowne zmiany w swojej organizacji. Pamiętaj również o korzystaniu z nowych rozwiązań. Producenci sprzętu komputerowego w produktach przeznaczonych dla firm stosują już różne narzędzia, takie jak ochronę BIOS-u czy możliwość sprawnego odzyskiwania danych. Istnieją również systemy pozwalające na śledzenie komputerów, które zostały ukradzione. Poszukaj również oprogramowania, które pozwala na dokładną weryfikację tego, co dzieje się na komputerach pracowników – nie chodzi tu oczywiście o ich śledzenie, ale o analizę tego, czy komputer nie został zainfekowany w ich domach, a następnie czy złośliwe oprogramowanie nie zostanie przeniesione do firmy. Cel powinien być jeden – maksymalizacja bezpieczeństwa i minimalizacja strat.

CO TO JEST ATAK I LUKA ZERO-DAY

To jeden z najgroźniejszych rodzajów ataku, gdyż wykorzystuje lukę w systemie, o której nie wie producent oprogramowania. Przed luką zero-day nie ma więc żadnej obrony, dopóki ktoś jej nie odkryje i nie przygotuje zabezpieczenia. W 2004 r. Izrael wykorzystał robaka typu zero-day do zatrzymania irańskiego programu nuklearnego.

PAMIĘTAJ, ŻE W ATAKACH PRZESTĘPCY CZĘSTO WYKORZYSTUJĄ ZNANE MARKI. W OSTATNIM KWARTALE 2021 R. BYŁY TO M.IN. DHL, MICROSOFT, WHATSAPP, GOOGLE I LINKEDIN. EKSPERCI ZWRACAJĄ UWAGĘ, ŻE W TEGO TYPU ATAKACH CORAZ CZĘŚCIEJ WYKORZYSTUJE SIĘ MEDIA SPOŁECZNOŚCIOWE

EKSPERT

Grzegorz Waszkiewicz
broker ubezpieczeniowy, członek zarządu Krajowego Biura Obsługi Roszczeń Ubezpieczeniowych, twórca portalu BezpieczenstwowBiznesie.pl

CYBERPOLISY

Szkody z tytułu cyberwłamań mogą mieć różny charakter. Jedne z nich to straty bezpośrednie poszkodowanej firmy takie jak nagłe wyłączenie, spowolnienie lub zablokowanie sieci komputerowej, utrata lub kradzież danych, szantaż, a w przypadku coraz częściej stosowanego internetu rzeczy blokada systemów i urządzeń. Takie włamanie najczęściej zatrzymuje fizyczne funkcjonowanie firmy lub jej klientów. Przykład: blokada zamków do hotelowych pokoi.

Drugi rodzaj strat to poszkodowane osoby trzecie: najczęściej ofiarami są klienci, dostawcy, współpracownicy, pracownicy, kontrahenci, których dane zostały skradzione. Roszczenia w formie odszkodowań, zadośćuczynień, kar i grzywien w granicach dozwolonych przez prawo mogą być kierowane przez nich samych i regulatora państwowego.

Po każdym takim wydarzeniu trzeba koniecznie przeprowadzić analizę przyczyn, ustalając i utrwalając dowody szkody. Następnie naprawić system i zabezpieczyć się na przyszłość. Czy można się przed tym wszystkim zabezpieczyć? Przed samym atakiem z pewnością nie. W znacznym stopniu można jednak ograniczyć straty. Koszty pokryją świadczenia z odpowiednich polis ubezpieczeniowych, które określane są jako cyberpolisy. Jednak należy sobie zdawać sprawę z ich konstrukcji. Pamiętajmy, że szkody wyrządzone komuś zabezpieczymy klauzulami cyber w polisach OC. Natomiast firmowe straty majątkowe łącznie z utratą zysku zabezpieczymy dodatkowymi klauzulami cyber w ubezpieczeniach mienia przedsiębiorstwa.