**Scenario**

Jesteś analitykiem cyberbezpieczeństwa pracującym dla firmy multimedialnej, która oferuje usługi projektowania stron internetowych, projektowanie graficzne i rozwiązania marketingowe w mediach społecznościowych dla małych firm. Twoja organizacja niedawno doświadczyła ataku DDoS, który naruszył sieć wewnętrzną na dwie godziny, zanim został rozwiązany.

Podczas ataku usługi sieciowe Twojej organizacji nagle przestały odpowiadać z powodu zalewu przychodzących pakietów ICMP. Normalny wewnętrzny ruch sieciowy nie mógł uzyskać dostępu do żadnych zasobów sieciowych. Zespół zarządzania incydentami zareagował, blokując przychodzące pakiety ICMP, zatrzymując wszystkie niekrytyczne usługi sieciowe w trybie offline i przywracając krytyczne usługi sieciowe.

Zespół ds. cyberbezpieczeństwa firmy zbadał następnie zdarzenie związane z bezpieczeństwem. Odkryli, że złośliwy aktor wysłał powódź pingów ICMP do sieci firmy przez nieskonfigurowaną zaporę ogniową. Ta luka umożliwiła złośliwemu atakującemu przytłoczenie sieci firmowej poprzez rozproszony atak typu „odmowa usługi” (DDoS).

Aby zaradzić temu zdarzeniu związanemu z bezpieczeństwem, zespół ds. bezpieczeństwa sieci wdrożył:

* Nowa reguła zapory ograniczająca szybkość przychodzących pakietów ICMP
* Weryfikacja źródłowego adresu IP na zaporze sieciowej w celu sprawdzenia, czy w przychodzących pakietach ICMP nie występują fałszywe adresy IP
* Oprogramowanie do monitorowania sieci do wykrywania nieprawidłowych wzorców ruchu
* System IDS/IPS do filtrowania ruchu ICMP na podstawie podejrzanych cech

Jako analityk ds. bezpieczeństwa cybernetycznego masz za zadanie wykorzystać to zdarzenie związane z bezpieczeństwem do stworzenia planu poprawy bezpieczeństwa sieci w Twojej firmie zgodnie z ramami bezpieczeństwa cybernetycznego (CSF) Narodowego Instytutu Standardów i Technologii (NIST). Będziesz korzystać z CSF, aby pomóc Ci przejść przez różne etapy analizy tego incydentu związanego z cyberbezpieczeństwem i zintegrować swoją analizę z ogólną strategią bezpieczeństwa:

* **Identyfikuj** zagrożenia bezpieczeństwa poprzez regularne audyty wewnętrznych sieci, systemów, urządzeń i uprawnień dostępu, aby zidentyfikować potencjalne luki w zabezpieczeniach.
* **Chroń** zasoby wewnętrzne poprzez wdrażanie zasad, procedur, szkoleń i narzędzi, które pomagają łagodzić zagrożenia cyberbezpieczeństwa.
* **Wykrywaj** potencjalne incydenty bezpieczeństwa i ulepszaj możliwości monitorowania, aby zwiększyć szybkość i skuteczność wykrywania.
* **Reaguj**, aby powstrzymać, zneutralizować i przeanalizować incydenty związane z bezpieczeństwem; wdrażać usprawnienia w procesie bezpieczeństwa.
* **Przywróć** systemy, których dotyczy problem, do normalnego działania i przywróć dane systemowe i/lub zasoby, które zostały dotknięte incydentem

**Materiały pomocnicze znajdziemy w folderze z scenariuszem**

**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

|  |  |
| --- | --- |
| **Summary** | Scenariusz… |
| Identify | Zespół ds. Cyberbezpieczeństwa organizacji odkrył że do ataku zastosowano atak typu DDoS ICMP flood attack. Złośliwi aktorzy wykorzystali powódź pakietów protokołu ICMP do przeciążenia zasobów sieci węwnetrznej. |
| Protect | Organizacja powinna skonfigurować zapory ogniowe oraz urządzenia sieciowe w celu blokowania pakietów ICMP z nieznanych adresów IP i sieci. Pakiety ICMP powinny być odbierane tylko ze znanych źródeł. |
| Detect | W celu wykrywania przyszłych ataków drużyna wprowadzi systemy IDS oraz IPS filtrujące ruch w sieci, te dane będą agregowane w narzędziach SIEM. |
| Respond | Systemy IPS powinny zablokować część znanych zachowań atakujących. Natomiast specjaliści wyposażeni w dane zebrane przez systemy IDS i IPS w narzędziu SIEM będą potrafili zareagować na podejrzane zachowania jeśli zostaną one zauważone. Na przyszłość drużyna wyizoluje systemy aby zapobiec dalszego rozprzestrzeniania się zakłóceń w sieci. |
| Recover | Aby przywrócić systemy po ataku DDoS, dostęp do serwisów sieci musi powrócić do normalnego stanu. Wszystkie niekrytyczne serwisy powinny zostać zatrzymane aby zmniejszyć wewnętrzny przepływ danych. Następnie krytyczne systemy muszą zostać przywrócone jako pierwsze, a po przerwaniu ICMP flood przywracać te niekrytyczne. |

|  |
| --- |
| Reflections/Notes: |