Управљање безбедношћу и ризицима

Принципи и кључни концепти управљања Информационом безбедношћу - Студија случаја

РЕШЕЊЕ



Бранко Суботић, Консултант

Студија случаја: Одговор на ransomware напад на производно предузеће

Компанија АБЦ, која се бави производњом прехрамбених производа широке потрошње, је доживела ransomware-а напад, који је криптовао већину критичних податке у различитим одељењима укључујући сегмент планирање производње, све финансијске податке и податке о интелектуалној својини у секторима дизајна, производње и маркетинга. Нападачи захтевају значајну откупнину у замену за кључеве за декрипцију.

У новонасталој ситуацији су између осталих активно укључени следеће функције:

1. Извршни Директор Компаније (CEO)
2. Директор за информациону безбедност (CISO)
3. Менаџери појединачних пословних функција (Власници процеса и података)
4. Управљачки одбор за ИТ (IT Steering Committee)

У наставку су приказане специфичне одговорности, питања и акције које произилазе из наведене ситуације, а нису додељене ниједној од наведених функција. Можете ли да наведене одговорности, питања и акције распоредите свакој од наведених функција, на начин на који мислите да најбоље одговара реалној ситуацији.

Студија случаја: Одговор на ransomware напад на производно предузеће

Одговорности:

1. Саветовање CEO-а и других извршних директора о техничким детаљима и опцијама опоравка.
2. Координација са ИТ особљем за сузбијање и ублажавање напада.
3. Генерално доношење одлука о плаћању откупнине.
4. Процена утицаја на специфичне пословне области.
5. Комуникација са заинтересованим странама и јавношћу.
6. Комуникација специфичних потреба и изазова Управљачком одбору за ИТ и CISO-у.
7. Обезбеђивање континуитета пословања.
8. Вођење техничког одговора на напад.
9. Пружање стратешког вођења политикама и праксама ИТ сигурности.
10. Сарадња са ИТ-ом за обнову пословних операција.
11. Надгледање развоја и имплементације стратегија опоравка.
12. Додела ресурса за ИТ сигурност и напоре опоравка.

Студија случаја: Одговор на ransomware напад на производно предузеће

Питања:

1. Која подршка је потребна од ИТ и сигурносних тимова?
2. Који су технички детаљи напада?
3. Да ли компанија треба да плати откупнину?
4. Које промене треба направити у политикама ИТ сигурности као резултат овог напада?
5. Како се напад може сузбити и ублажити?
6. Које опције опоравка су доступне?
7. Које су приоритети за обнову операција?
8. Како треба комуницирати информације о нападу са заинтересованим странама и јавношћу?
9. Које хитне акције треба предузети да се обезбеди континуитет пословања?
10. Како треба доделити ресурсе за напоре опоравка?
11. Какав је утицај на операције мог одељења?
12. Које дугорочне стратегије треба имплементирати да се спрече будући напади?

Студија случаја: Одговор на ransomware напад на производно предузеће

Акције (одговори):

1. Покретање плана за хитне ситуације који укључује алтернативне методе производње и привремене финансијске мере.
2. Пружање детаљне анализе варијанте ransomware-а и коришћеног вектора напада.
3. Спровођење мера за изолацију заражених система како би се спречило ширење.
4. Одобравање стратегије комуникације развијене у координацији са одељењем за односе с јавношћу за управљање јавним перцепцијама и умиривање заинтересованих страна.
5. Развијање плана опоравка користећи резервне копије, ако су доступне, или истраживање техника дешифровања ако се откупнина не плати.
6. Додељивање повећаног финансирања за сигурносне алате, обуку особља и надоградњу инфраструктуре.
7. Приоритизација обнове кључних операција као што су обрада наруџбина и планирање производње.

Студија случаја: Одговор на ransomware напад на производно предузеће

Акције (одговори):

8. Захтевање специфичне техничке подршке и сигурносних мера како би се осигурало да обновљени системи буду сигурни.
9. Детаљно објашњење степена губитка података и поремећених процеса.
10. Препорука ажурирања сигурносних политика укључујући чешће резервне копије, појачани мониторинг и обуку запослених о фишингу.
11. Процена импликација плаћања наспрам неплаћања откупнине са Управљачким одбором за ИТ и правним саветницима.
12. Развијање дугорочног плана који укључује редовне сигурносне ревизије, усвајање напредних алата за детекцију претњи и побољшани протокол за реаговање на инциденте.

Студија случаја: Одговори полазника

Извршни Директор Компаније (CEO)

Одговорности:

Генерално доношење одлука о плаћању откупнине.
Комуникација са заинтересованим странама и јавношћу.
Обезбеђивање континуитета пословања.

Питања:

Да ли компанија треба да плати откупнину?
Како треба комуницирати информације о нападу са заинтересованим странама и јавношћу?
Које хитне акције треба предузети да се обезбеди континуитет пословања?

Акције (одговори):

Процена импликација плаћања наспрам неплаћања откупнине са Управљачким одбором за ИТ и правним саветницима.
Одобравање стратегије комуникације развијене у координацији са одељењем за односе с јавношћу за управљање јавним перцепцијама и умиривање заинтересованих страна.
Покретање плана за хитне ситуације који укључује алтернативне методе производње и привремене финансијске мере.

Студија случаја: Одговори полазника

Директор за информациону безбедност (CISO)

Одговорности:

Вођење техничког одговора на напад.
Координација са ИТ особљем за сузбијање и ублажавање напада.
Саветовање CEO-а и других извршних директора о техничким детаљима и опцијама опоравка.

Питања:

Који су технички детаљи напада?
Како се напад може сузбити и ублажити?
Које опције опоравка су доступне?

Акције (одговори):

Пружање детаљне анализе варијанте ransomware-а и коришћеног вектора напада.

Спровођење мера за изолацију заражених система како би се спречило ширење.

Развијање плана опоравка користећи резервне копије, ако су доступне, или истраживање техника дешифровања ако се откупнина не плати.

Студија случаја: Одговори полазника

Менаџери појединачних пословних функција (Власници процеса и података)

Одговорности:

Процена утицаја на специфичне пословне области.
Сарадња са ИТ-ом за обнову пословних операција.
Комуникација специфичних потреба и изазова Управљачком одбору за ИТ и CISO-у

Питања:

Какав је утицај на операције мог одељења?
Које су приоритети за обнову операција?
Која подршка је потребна од ИТ и сигурносних тимова?

Акције (одговори):

Детаљно објашњење степена губитка података и поремећених процеса.

Приоритизација обнове кључних операција као што су обрада наруџбина и планирање производње.

Захтевање специфичне техничке подршке и сигурносних мера како би се осигурало да обновљени системи буду сигурни.

Студија случаја: Одговори полазника

Управљачки одбор за ИТ (IT Steering Committee)

Одговорности:

Пружање стратешког вођења политикама и праксама ИТ сигурности.
Надгледање развоја и имплементације стратегија опоравка.
Додела ресурса за ИТ сигурност и напоре опоравка.

Питања:

Које промене треба направити у политикама ИТ сигурности као резултат овог напада?
Како треба доделити ресурсе за напоре опоравка?
Које дугорочне стратегије треба имплементирати да се спрече будући напади?

Акције (одговори):

Препорука ажурирања сигурносних политика укључујући чешће резервне копије, појачани мониторинг и обуку запослених о фишингу.

Додељивање повећаног финансирања за сигурносне алате, обуку особља и надоградњу инфраструктуре.

Развијање дугорочног плана који укључује редовне сигурносне ревизије, усвајање напредних алата за детекцију претњи и побољшани протокол за реаговање на инциденте.