

REFERENCA: PROTOKOLLET E PERGJIGJES

FAZA 1: IDENTIFIKIMI

Kohezgjatja: 0-2 orë

Objektivat:

- Konfirmoni që ka ndodhur shkelje
- Vlerësoni shkallën fillestare
- Identifikoni sistemet e prekura
- Aktivizoni ekipin e reagimit

Pyetjet Kyc:

- ? Çfarë sistemi u prek?
- ? Kur filloi incidenti?
- ? Sa rekorde janë potencialisht të ekspozuara?
- ? A është aktiv ende sulmi?

FAZA 2: IZOLIMI

Kohezgjatja: 2-6 orë

Objektivat:

- Ndaloni përhapjen e sulmit
- Izoloni sistemet e prekura
- Ruani provat dixhitale
- Aktivizoni sistemet backup

Pyetjet Kyc:

- ? A janë izoluar sistemet e prekura?
- ? A kemi backup të sigurt?
- ? A janë ruajtur log-et?
- ? A mund të vazhdojnë operacionet kritike?

FAZA 3: ELIMINIMI

Kohezgjatja: 6-24 orë

Objektivat:

- Hiqni malware/aksesin e paautorizuar
- Mbyllni vulnerabilitetin

- Rivendosni kredencialet
- Verifikoni pastrimin

Pyetjet Kyc:

- ? A është hequr kërcënimi?
- ? A është mbyllur vektori i sulmit?
- ? A janë ndryshuar të gjitha kredencialet?
- ? A jemi të sigurt për riaktivizim?

FAZA 4: RIKUPERIMI

Kohezgjatja: 24-72 orë

Objektivat:

- Rivendosni sistemet nga backup i sigurt
- Testoni funksionalitetin
- Monitoroni për ri-infektim
- Riaktivizoni shërbimet

Pyetjet Kyc:

- ? A janë rivendosur sistemet?
- ? A funksionon gjithçka normalisht?
- ? A kemi monitorim të shtuar?
- ? A janë njoftuar palët e interesuara?

FAZA 5: MËSIMET

Kohezgjatja: 1-4 javë pas

Objektivat:

- Dokumentoni incidentin plotësisht
- Analizoni shkaqet rrënjësore
- Identifikoni përmirësimet
- Përditësoni procedurat

Pyetjet Kyc:

- ? Si hyri sulmuesi?
- ? Çfarë dështoi në mbrojtje?
- ? Si mund ta parandalojmë në të ardhmen?
- ? A nevojiten trajnime të reja?

PERMBAJTJA E NJOFTIMEVE

AKCESK - Autoriteti Kombëtar i Certifikimit Elektronik dhe Sigurisë Kibernetike

Afati: 72 orë

Permbajtja:

- Natyra e shkeljes
- Kategoritë e të dhënave
- Numri i të prekurve
- Masat e marra

KMDP - Komisioneri për Mbrojtjen e të Dhënave Personale

Afati: 72 orë

Permbajtja:

- Përshkrimi i shkeljes
- Kontakti DPO
- Pasojat e mundshme
- Masat korrigjuese

SUBJEKTET - Individët e Prekur

Afati: Pa vonesë të pajustificuar

Permbajtja:

- Çfarë ndodhi
- Çfarë të dhënash u prekën
- Çfarë po bëjmë
- Çfarë duhet të bëni ju

POLICIA - Policia e Shtetit / Prokuroria

Afati: Menjëherë

Permbajtja:

- Raporti i incidentit
- Provat dixhitale
- Dëshmitë
- Dëmi i shkaktuar