KARTAT E SKENAREVE

Pritini dhe shperndani - nje per ekip

[BREACH-01] Sulm Ransomware ne Serverin e Pasaportave

Serioziteti: KRITIK

Kategoria: Malware/Ransomware

PERSHKRIMI:

```
Ora 09:15 - Sistemi i lëshimit të pasaportave nuk përgjigjet.
Ora 09:22 - Ekrani tregon mesazh: "Të dhënat tuaja janë enkriptuar. Paguani 50 BTC."
Ora 09:30 - IT konfirmon: 3 serverë janë të infektuar.
Ora 09:45 - Zbulohet: 150,000 rekorde pasaportash potencialisht të ekspozuara.
```

Sistemet e prekura: Serveri i pasaportave, Databaza e aplikimeve, Backup lokal

Te dhenat ne rrezik: Emra dhe mbiemra, Foto biometrike, Numra pasaportash, Data lindje, Adresa

Rekorde te ekspozuara: 150,000

Koha per pergjigje: 72 ore

- - - - - - PRITNI KETU - - - - - -

[BREACH-02] Akses i Paautorizuar nga Punonjës

Serioziteti: I LARTË

Kategoria: Kërcënim i Brendshëm

PERSHKRIMI:

```
Ora 14:00 - Auditi zbulon: Një punonjës ka aksesuar 5,000 rekorde pa autorizim.
Ora 14:30 - Log-et tregojnë eksport të të dhënave në USB.
Ora 15:00 - Punonjësi nuk gjendet në zyrë.
Ora 15:30 - Kamerat konfirmojnë daljen e tij me laptop personal.
```

Sistemet e prekura: Sistemi i Gjendjes Civile, Terminali i punonjësit

Te dhenat ne rrezik: NID, Certifikata lindje, Adresa, Lidhje familjare

Rekorde te ekspozuara: 5,000

Koha per pergjigje: 24 ore

- - - - - - PRITNI KETU - - - - - -

[BREACH-03] Rrjedhje nga Backup i Pakonfiguruar

Serioziteti: I LARTË

Kategoria: Konfigurim i Gabuar

PERSHKRIMI:

```
Ora 10:00 - Kërkues sigurie raporton: Backup i databazës i aksesueshëm publikisht.
Ora 10:15 - Konfirmojmë: S3 bucket pa autentikim për 14 ditë.
Ora 10:30 - Analizojmë log-et: 23 IP të ndryshme kanë shkarkuar të dhëna.
Ora 11:00 - Madhësia e backup: 2.3 GB me 80,000 rekorde.
```

Sistemet e prekura: AWS S3 Bucket, Sistemi i backup

Te dhenat ne rrezik: Të dhëna pasaportash, Foto, Historik aplikimesh, Shënime interne

Rekorde te ekspozuara: 80,000

Koha per pergjigje: 48 ore

- - - - - - PRITNI KETU - - - - - -

[BREACH-04] Sulm Phishing ndaj Administratorëve

Serioziteti: KRITIK

Kategoria: Inxhinieri Sociale

PERSHKRIMI:

```
Ora 08:00 - Admin merr email "urgjent" nga "Drejtori IT".
Ora 08:05 - Admin klikon linkun dhe fut kredencialet.
Ora 08:10 - Sulmuesi fiton akses admin në sistemin e ID-ve.
Ora 11:00 - Zbulohet: 3 orë akses i pakontrolluar në sistem.
Ora 11:30 - Konfirmojmë: 25,000 rekorde të shikuara, 500 të eksportuara.
```

Sistemet e prekura: Sistemi i Kartave të Identitetit, Active Directory, Email server

Te dhenat ne rrezik: Foto ID, NID, Adresa, Nënshkrime dixhitale

Rekorde te ekspozuara: 25,000

Koha per pergjigje: 24 ore

- - - - - - PRITNI KETU - - - - - -

[BREACH-05] Humbja e Laptopit me të Dhëna

Serioziteti: MESATAR

Kategoria: Humbje Fizike

PERSHKRIMI:

```
Ora 18:00 - Punonjësi raporton: Laptopi u vodh nga makina.
Ora 18:30 - Konfirmojmë: Laptopi kishte kopje lokale të 2,000 aplikimeve.
Ora 19:00 - IT kontrollon: Disku NUK ishte i enkriptuar.
Ora 19:30 - Aplikime përmbajnë: foto, NID, certifikata, adresa.
```

Sistemet e prekura: Laptop punonjësi, Kopja lokale e databazës

Te dhenat ne rrezik: Aplikime pasaportash, Foto, Dokumente mbështetëse, Korrespondencë

Rekorde te ekspozuara: 2,000

Koha per pergjigje: 72 ore

- - - - - - PRITNI KETU - - - - - -