# Kampen mod cybermørket – Awareness-spillet

## Antal Spillere:

4 spillere, hvor hver spiller repræsenterer en virksomhed.

## Materialer:

Spillebræt
42 sikkerhedskort (blå)
20 angrebskort (røde)
24 chancekort (gule)
Aktiekurspoint (forskellige farver)
Kryptocoins (orange)

Derudover skal der medbringes:
Spillebrikker eller post-its i 4 farver
Sakse
Terning

## Historien bag

Velkommen til spillet, hvor nystartede virksomheder dyster om at opbygge den mest sikre og profitable forretning. Men pas på! Trusler som hacking, phishing og interne sårbarheder lurer overalt. Kan du navigere gennem disse udfordringer og klare kampen mod cybermørket?

## Mål:

Formålet er at opnå så høj aktiekurs som muligt, mens man opretholder en god IT-sikkerhed.

## Sådan spiller I:

1. Opstart:
    a. Læg sikkerhedskortene (blå) på brættet med billedsiden opad
    b. Bland chancekortene (gule) og læg dem på brættet med billedsiden nedad
    c. Bland angrebskortene (røde) og læg dem på brættet med billedsiden nedad
    d. Placer kryptocoins og aktiekurspoint i deres felter på brættet
    e. Hver spiller vælger en virksomhedsbrik og placerer den på startfeltet.
    f. Hver spiller modtager 100 aktiekurspoint og 3 kryptocoins.
    g. Hver spiller har mulighed for at købe et sikkerhedskort med værdien 1kryptocoin
2. Spillet
    a. START: Kast terningen for at afgøre, hvem der begynder. Den spiller, der slår lavest, skal begynde.
    b. FLYTNING: Kast terningen for at bevæge brikken det antal øjne, som terningen viser.
    c. HANDLING: Handlingen afhænger af hvilket felt, spilleren lander på. Læs altid kortene højt.:

i. Blåt: Sikkerhedsfelt. Spilleren kan vælge at købe et sikkerhedskort. Kortene betales med kryptocoins, og prisen står på kortet. Hvert sikkerhedskort beskytter mod 2-6 typer it-angreb. Spilleren kan frit vælge, hvilket ledigt sikkerhedskort han/hun evt. vil købe.

ii. Rødt: Angrebskort: Spilleren trækker et angrebskort
    1. Spilleren læser navnet på kortet højt, samt hvordan angrebet virker.
    2. OBS! Nogle angreb kan ramme alle virksomheder på én gang. Dette fremgår øverst på kortet.
    3. Hvis spillerens virksomhed rammes, kan spilleren bruge sine sikkerhedskort til at afværge angrebet.
        a. Det fremgår af sikkerhedskortene, hvilke angreb, de beskytter imod.
        b. Hvis spilleren har et sikkerhedskort, som afværger angrebet, vil spilleren modtage en bonus. Størrelsen af bonus fremgår af angrebskortet.
        c. Hvis spilleren ikke har et sikkerhedskort, som afværger angrebet, skal spilleren betale de omkostninger, der fremgår af angrebskortet
        d. Spilleren beholder sikkerhedskortet, når det har været i brug, og det kan benyttes igen
    4. Behold brugte angrebskort

iii. Gult: Chancekort. Spilleren trækker et chancekort og følger anvisningen på kortet. Brugte kort lægges i bunden af stakken med chancekort

iv. Orange: Kryptocoinfelt. Spilleren tager på it-sikkerhedskursus og modtager en kryptocoin.


v. Grønt:
    1. Startfelt: Spilleren modtager 50 aktiekurspoint og 2 kryptocoins, når han/hun lander på eller passerer start
    2. Halvårsregnskab: Spilleren modtager 25 aktiekurspoint, når han/hun lander på eller passerer halvårsregnskabsfeltet.

3. Konkurs: Hvis spillerens samlede aktiekurspoint er under 0, er spilleren gået konkurs og udgår af spillet.
4. Afslutning: Spillet slutter, når den første spiller har passerets målfeltet for anden gang.
5. Vinderen: Vinderen er den virksomhed, som har den højeste aktiekursværdi:
    a. Hvert sikkerhedskort har en værdi af pris x 10 aktiekurspoint. Eksempel: Hvis sikkerhedskortet koster 2 kryptocoins, har den en værdi på 20 aktiekurspoint.
    b. Kryptocoins har ingen værdi, når spillet er slut
    c. Optæl det samlede antal aktiekurspoint

## ANTI-PHISHING TRÆNING

Uddanner medarbejdere i at genkende phishing-forsøg

**Forsvarer mod følgende angreb**

Phishingangreb
Spoofing
Data Leak
Ransomware

**Pris**
2 Kryptocoins

## AUTOMATISK BACKUP

Skaber automatiske kopier af data for at forhindre datatab.

**Forsvarer mod følgende angreb**

Ransomware
Malware
Insider threat
SQL Injection

**Pris**
2 Kryptocoins

## BIOMETRISK ADGANG

Bruger fysiologiske træk som fingeraftryk eller ansigtsgenkendelse for at give adgang

**Forsvarer mod følgende angreb**

Credential Stuffing
Brute force

**Pris**
1 Kryptocoin

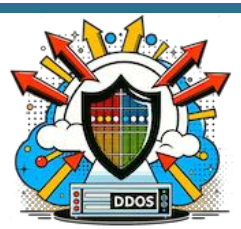
## DATA MASKERING

Skjuler følsomme data med tilfældige tegn

**Forsvarer mod følgende angreb**

Data Leak
SQL Injection
XSS Attack
Man-in-the-middle

**Pris**
2 Kryptocoins




## DDoS BESKYTTELSE

Filtrerer og omdirigerer skadelig trafik under DDoS-angreb

**Forsvarer mod følgende angreb**

DDoS Angreb
Zero-Day exploit

**Pris**
1 Kryptocoin

## ENDPOINT SECURITY

Beskytter netværksendepunkter som computere og mobile enheder mod skadelige aktiviteter

**Forsvarer mod følgende angreb**

Zero-Day Exploit
Rootkit
Watering Hole
XSS Attack
Eavesdropping
Clickjacking

**Pris**
3 Kryptocoins

## FIREWALL

Blokerer eller tillader netværkstrafik baseret på sikkerhedsregler.

**Forsvarer mod følgende angreb**

Intern Hacking
DDoS Angreb
Malware
Phishingangreb
Ransomware
SQL Injection

**Pris**
3 Kryptocoins

## IDS

Overvåger netværk for tegn på mulige indtrængen og sender advarsler, når det sker

**Forsvarer mod følgende angreb**

Intern Hacking
DDoS Angreb
Eavesdropping
Clickjacking

**Pris**
2 Kryptocoins

## INCIDENT RESPONSE TEAM

Et dedikeret team, som er klar til hurtigt at reagere på sikkerhedsbrud

**Forsvarer mod følgende angreb**
Phishingangreb
Insider threat
Spoofing
Social engineering

**Pris**
2 Kryptocoins


## KRYPTERING

Omdanner almindelig tekst til kode for at beskytte data

**Forsvarer mod følgende angreb**
Ransomware
Spoofing

**Pris**
2 Kryptocoins

## LOG ANALYSE

Overvågning og analyse af system-logs for at opdage usædvanlige eller mistænkelige aktiviteter.

**Forsvarer mod følgende angreb**
Credential Stuffing
Man-in-the-middle

**Pris**
1 Kryptocoin

## MULTI-FAKTOR AUTENTIFIKATION

Kræver to eller flere former for bevis for at validere en brugers identitet

**Forsvarer mod følgende angreb**
Data Leak
Social engineering
SQL Injection
Credential stuffing

**Pris**
2 Kryptocoins


## PASSWORD MANAGER

Software, der genererer og opbevarer komplekse adgangskoder, så brugerne ikke behøver at huske dem

**Forsvarer mod følgende angreb**
Keylogger
Credential stuffing

**Pris**
1 Kryptocoin

## PATCH MANAGEMENT

Håndterer softwareopdateringer og rettelser.

**Forsvarer mod følgende angreb**
XSS Attack
Zero-day exploit

**Pris**
1 Kryptocoin

## RED TEAM ØVELSER

Simulerede angreb på organisationens netværk for at teste dets forsvarsmekanismer

**Forsvarer mod følgende angreb**
Social Engineering
SQL Injection
Phishingangreb
Man-in- the-middle

**Pris**
2 Kryptocoins

REMOTE WIPE

Kan fjerne data fra en fjernenhed for at beskytte mod uautoriseret adgang

**Forsvarer mod følgende angreb**
Insider Threat
Rootkit

**Pris**
1 Kryptocoin

SIKKER EMAIL GATEWAY

Filtrerer e-mails for at opdage og blokere trusler.

**Forsvarer mod følgende angreb**
Clickjacking
Keylogger

**Pris**
1 Kryptocoin


VPN

Skaber en sikker, krypteret forbindelse for internetadgang.

**Forsvarer mod følgende angreb**
Eavesdropping
Watering hole

**Pris**
1 Kryptocoin

WHITELISTING

Tillader kun godkendte applikationer at køre på et netværk eller en enhed.

**Forsvarer mod følgende angreb**
Malware
Rootkit
Spoofing
Watering hole

**Pris**
2 Kryptocoins

ZERO TRUST ARKITEKTUR

Ingen brugere eller systemer er betroede per automatik; alle skal verificeres.

**Forsvarer mod følgende angreb**
Insider Threat
Intern hacking
Data Leak
Social engineering
Man-in-the-Middle
Spoofing

**Pris**
3 Kryptocoins

INGEN IT-SIKKERHEDS-INVESTERING

Du vælger ikke at investerer i IT-sikkerhed i denne tur.
Da du sparer penge i virksomheden på kort sigt, får du en umiddelbar kursgevinst på 15 point.

**Pris**
1 Kryptocoin

Skal ikke bruges

Skal ikke bruges

Skal ikke bruges

## ANTI-PHISHING TRÆNING

Uddanner medarbejdere i at genkende phishing-forsøg

**Forsvarer mod følgende angreb**

Phishingangreb
Spoofing
Data Leak
Ransomware

**Pris**
2 Kryptocoins

## AUTOMATISK BACKUP

Skaber automatiske kopier af data for at forhindre datatab.

**Forsvarer mod følgende angreb**

Ransomware
Malware
Insider threat
SQL Injection

**Pris**
2 Kryptocoins

## BIOMETRISK ADGANG

Bruger fysiologiske træk som fingeraftryk eller ansigtsgenkendelse for at give adgang

**Forsvarer mod følgende angreb**

Credential Stuffing
Brute force

**Pris**
1 Kryptocoin

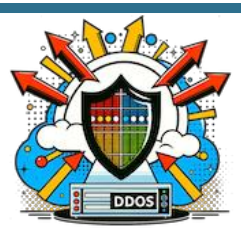
## DATA MASKERING

Skjuler følsomme data med tilfældige tegn

**Forsvarer mod følgende angreb**

Data Leak
SQL Injection
XSS Attack
Man-in-the-middle

**Pris**
2 Kryptocoins




## DDoS BESKYTTELSE

Filtrerer og omdirigerer skadelig trafik under DDoS-angreb

**Forsvarer mod følgende angreb**

DDoS Angreb
Zero-Day exploit

**Pris**
1 Kryptocoin

## ENDPOINT SECURITY

Beskytter netværksendepunkter som computere og mobile enheder mod skadelige aktiviteter

**Forsvarer mod følgende angreb**

Zero-Day Exploit
Rootkit
Watering Hole
XSS Attack
Eavesdropping
Clickjacking

**Pris**
3 Kryptocoins

## FIREWALL

Blokerer eller tillader netværkstrafik baseret på sikkerhedsregler.

**Forsvarer mod følgende angreb**

Intern Hacking
DDoS Angreb
Malware
Phishingangreb
Ransomware
SQL Injection

**Pris**
3 Kryptocoins

## IDS

Overvåger netværk for tegn på mulige indtrængen og sender advarsler, når det sker

**Forsvarer mod følgende angreb**

Intern Hacking
DDoS Angreb
Eavesdropping
Clickjacking

**Pris**
2 Kryptocoins

## INCIDENT RESPONSE TEAM

Et dedikeret team, som er klar til hurtigt at reagere på sikkerhedsbrud

**Forsvarer mod følgende angreb**
Phishingangreb
Insider threat
Spoofing
Social engineering

**Pris**
2 Kryptocoins


## KRYPTERING

Omdanner almindelig tekst til kode for at beskytte data

**Forsvarer mod følgende angreb**
Ransomware
Spoofing

**Pris**
2 Kryptocoins

## LOG ANALYSE

Overvågning og analyse af system-logs for at opdage usædvanlige eller mistænkelige aktiviteter.

**Forsvarer mod følgende angreb**
Credential Stuffing
Man-in-the-middle

**Pris**
1 Kryptocoin

## MULTI-FAKTOR AUTENTIFIKATION

Kræver to eller flere former for bevis for at validere en brugers identitet

**Forsvarer mod følgende angreb**
Data Leak
Social engineering
SQL Injection
Credential stuffing

**Pris**
2 Kryptocoins


## PASSWORD MANAGER

Software, der genererer og opbevarer komplekse adgangskoder, så brugerne ikke behøver at huske dem

**Forsvarer mod følgende angreb**
Keylogger
Credential stuffing

**Pris**
1 Kryptocoin

## PATCH MANAGEMENT

Håndterer softwareopdateringer og rettelser.

**Forsvarer mod følgende angreb**
XSS Attack
Zero-day exploit

**Pris**
1 Kryptocoin

## RED TEAM ØVELSER

Simulerede angreb på organisationens netværk for at teste dets forsvarsmekanismer

**Forsvarer mod følgende angreb**
Social Engineering
SQL Injection
Phishingangreb
Man-in- the-middle

**Pris**
2 Kryptocoins

REMOTE WIPE

Kan fjerne data fra en fjernenhed for at beskytte mod uautoriseret adgang

**Forsvarer mod følgende angreb**
Insider Threat
Rootkit

**Pris**
1 Kryptocoin

SIKKER EMAIL GATEWAY

Filtrerer e-mails for at opdage og blokere trusler.

**Forsvarer mod følgende angreb**
Clickjacking
Keylogger

**Pris**
1 Kryptocoin


VPN

Skaber en sikker, krypteret forbindelse for internetadgang.

**Forsvarer mod følgende angreb**
Eavesdropping
Watering hole

**Pris**
1 Kryptocoin

WHITELISTING

Tillader kun godkendte applikationer at køre på et netværk eller en enhed.

**Forsvarer mod følgende angreb**
Malware
Rootkit
Spoofing
Watering hole

**Pris**
2 Kryptocoins

ZERO TRUST ARKITEKTUR

Ingen brugere eller systemer er betroede per automatik; alle skal verificeres.

**Forsvarer mod følgende angreb**
Insider Threat
Intern hacking
Data Leak
Social engineering
Man-in-the-Middle
Spoofing

**Pris**
3 Kryptocoins

INGEN IT-SIKKERHEDS-INVESTERING

Du vælger ikke at investerer i IT-sikkerhed i denne tur.
Da du sparer penge i virksomheden på kort sigt, får du en umiddelbar kursgevinst på 15 point.

**Pris**
1 Kryptocoin

Skal ikke bruges

Skal ikke bruges

Skal ikke bruges

## NYANSÆTTELSE

Du ansætter en dygtig IT-sikkerhedsekspert og får derfor en ekstra tur.

Slå straks med terningen.

Du modtager også 25 aktiekurspoint

## FINANSIEL BONUS

Dine aktier klarer sig godt.

Du modtager 30 aktiekurspoint.

## SIKKERHEDS-AUDIT

Eksterne konsulenter gennemgår virksomhedens IT-sikkerhed. Din virksomhed klarer sig godt.

Vælg et gratis sikkerhedskort til en værdi af 1 kryptocoin.

Du modtager også 10 aktiekurspoint

## WHISTLEBLOWER

Din virksomhed får en insider-information, der forhindrer det næste it-angreb.

Gem kortet til næste gang, din virksomhed udsættes for angreb.

Du modtager også 20 aktiekurspoint med det samme.


## GOD PRESSE

Sikkerhedstiltagene i din virksomhed, booster virksomhedens omdømme.

Du får immunitet næste tur, så du ikke kan blive ramt af angreb. Gem kortet indtil du har spillet næste tur.

Du modtager også 20 aktiekurspoint med det samme

## BØDE

Din virksomhed har ikke overholdt GDPR-reglerne og modtager derfor en bøde, der får aktiekurserne til at falde.

Du mister 10 aktiekurspoint.


## DÅRLIG PRESSE

Din virksomhed er udsat for et alvorligt hackerangreb, som afslører mangler i virksomhedens IT-sikkerhed. Det giver dårlig presseomtale.

Du mister næste tur, da du har travlt med at håndtere pressen.

## OPSIGELSE

En af dine dygtige IT-medarbejdere har sagt op pga. manglende udviklingsmuligheder i virksomheden.

Du mister næste tur, da du har travlt med at ansætte en ny medarbejder.

## PHISHING

En regnskabsmedarbejder falder for et phishingforsøg og sender et større pengebeløb til en ukendt svindler.

Du mister et valgfrit sikkerhedskort.

## MANGLENDE OPDATERING

Din virksomheds IT-sikkerhedssystemer er ikke opdaterede. Det bliver udnyttet af hackere.

Næste gang, du lander på et angrebsfelt, skal du trække to angrebskort.
Gem kortet indtil da.


## GENBRUG AF ADGANGSKODER

Mange medarbejdere i din virksomhed bruger den samme adgangskode til forskellige tjenester. Det udgør en meget stor risiko for, at en hacker kan få adgang til mange systemer, hvis en adgangskode bliver lækket.

Du skal springe en omgang over, mens du får styr på IT-sikkerheden.

## MANGLENDE BACKUP

Din virksomhed laver ikke løbende sikkerhedskopier af den kritiske data. Det gør virksomheden sårbar overfor tab af værdifulde og forretningskritiske data.

Du mister 10 aktiekurspoint.
OBS! Hvis du har sikkerhedskortet ”Automatisk Backup” mister du ikke point.


## STORMFLOD

En stormflod rammer landet og giver vand i virksomhedens serverrum.

It-afdelingen skal bruge mange ressourcer på at håndtere situationen, og du mister en kryptocoin.

## PRISUDDELING

Din virksomhed får en branche-pris for god it-sikkerhed, hvilket øger medarbejdernes moral.

Næste gang, du lander på et angrebsfelt, skal du ikke trække et angrebskort. Gem kortet indtil da.
Du modtager også 20 aktiekurspoint.

## NY SIKKERHEDS-TEKNOLOGI

Et gennembrud i virksomhedens forskningsafdeling giver virksomheden en ekstra forsvarsmekanisme mod en ny type malware.

Du modtager et gratis sikkerhedskort til en værdi af 1 kryptocoin.
Du modtager også 15 aktiekurspoint.

## SAMARBEJDE MED KONKURRENTER

I indgår i et samarbejde om at forbedre it-sikkerheden i branchen. Det bliver en succes.

Næste gang det lykkes dig at afværge et angreb med et sikkerhedskort, vil du modtage dobbelt bonus.
Gem kortet indtil da.

## BÆREDYTIGHED

Din virksomhed får positiv omtale i medierne for sine bæredygtighedstiltag. Det får aktiekursen til at stige.

Modtag 20 aktiekurspoint.

## DÅRLIGT OVERBLIK

En gennemgang af IT-sikkerheden afslører, at der mangler overblik over de mest kritiske data og systemer, som bør beskyttes i din virksomhed.

Du mister 1 kryptocoin.

## MANGLENDE TO-FAKTOR LOGIN

Din virksomhed benytter sig ikke af to-faktor login. Det gør medarbejdernes digitale færden mere usikker.

Du skal springe en omgang over, mens du får styr på IT-sikkerheden.
OBS! Hvis du har sikkerhedskortet ” Multifactor Authentication” skal du ikke springe en omgang over.


## SVAGE ADGANGSKODER

Flere medarbejdere bruger for svage adgangskoder. Det øger risikoen for, at virksomheden bliver hacket.

Næste gang, du lander på et angrebsfelt, skal du trække to angrebskort.
Gem kortet indtil da.


## GDPR-KURSUS

Alle medarbejdere har gennemført et online GDPR-kursus.

Modtag 10 aktiekurspoint.

## SoMe-KAMPAGNE

Din virksomhed har stor succes med en morsom kampagne på de sociale mediier.

Modtag 15 aktiekurspoint

## PRODUKTUDVIKLING

Din virksomhed lancerer et nyt banebrydende produkt.

Modtag 15 aktiekurspoint

## EFFEKTIVITET

Din virksomhed indfører nye tiltag i produktionen, som reducerer omkostninger og forbedrer driftseffektivitet.

Modtag 15 aktiekurspoint

## SPØRGSMÅL TIL DIN NABO TIL HØJRE

Hvor lang tid tager det teoretisk for en hacker at bryde dette password?: G5jDh40PgD&

A) 35 minutter
B) 4 dage
C) 41 år

Hvis din nabo svarer rigtigt, skal han/hun rykke 2 felter frem.

Svar: C) 41 år

## SPØRGSMÅL TIL DIN NABO TIL VENSTRE

Hvad kaldes det, når man forsøger at lokke folk til at give personlige oplysninger via falske e-mails?

A) Pswimming
B) Hunting
C) Phishing

Hvis din nabo svarer rigtigt, skal han/hun rykke 1 felt frem.

Svar: C) Phishing

## SPØRGSMÅL TIL DIN NABO TIL HØJRE

Hvad kaldes software, der gør destruktive eller uønskede ting på din computer, eksempelvis ved brug af virus.

A) Wall-ware
B) Malware
C) Event manager

Hvis din nabo svarer rigtigt, skal han/hun rykke 3 felter frem.

Svar: B) Malware

## SPØRGSMÅL TIL DIN NABO TIL HØJRE

Hvilken sikkerhedsforanstaltning bør din virksomhed som minimum investere i uanset størrelse?

A) Krypteringsteknologi
B) Antivirus
C) Data discovery

Hvis din nabo svarer rigtigt, skal han/hun rykke 2 felter frem.

Svar: B) Antivirus

## SPØRGSMÅL TIL DIN NABO TIL VENSTRE

Hvor lang tid tager det teoretisk for en hacker at bryde dette password?: H2Gj4f

A) 1 sekund
B) 2 minutter
C) 4 timer

Hvis din nabo svarer rigtigt, skal han/hun rykke 1 felt frem.

Svar: A) 1 sekund, da det kun indeholder 6 tegn

## SPØRGSMÅL TIL DIN NABO TIL HØJRE

Hvilken vigtig funktion har et VPN?

A) At øge netværkets hastighed
B) At skabe en sikker og krypteret forbindelse over internettet
C) At administrere brugerkonti og adgangsrettigheder

Hvis din nabo svarer forkert, skal han/hun rykke 1 felt tilbage.

Svar: B) At skabe en sikker og krypteret forbindelse over internettet

## SPØRGSMÅL TIL DIN NABO TIL VENSTRE

Hvilken af følgende typer angreb anses for at være en form for social engineering?

A) Brute force-angreb
B) Phishing
C) DDoS-angreb

Hvis din nabo svarer rigtigt, modtager han/hun 15 aktiekurspoint.

Svar: B) Phishing

## SPØRGSMÅL TIL DIN NABO TIL HØJRE

Hvordan bliver virksomheden bedst klædt på i kampen mod cybertruslen?

A) Køber nye arbejdscomputere
B) Underviser i hackingmetoder
C) Lærer alle medarbejdere om sikker adfærd online

Hvis din nabo svarer rigtigt, skal han/hun rykke 2 felter frem.

Svar: C) Lærer alle medarbejdere om sikker adfærd online

## INSIDER THREAT

En medarbejder bringer utilsigtet virksomhedens sikkerhed i fare, da han deler følsomme data med uvedkommende.

**Tab ved angreb**
Din virksomhed taber 20 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## DATA LEAK

Hackere har hacket sig adgang til din virksomheds data, og disse data er blevet delt.

**Tab ved angreb**
Din virksomhed taber 30 aktiekurspoint

**Bonus ved vellykket forsvar:**
2 Kryptocoins

## MAN-IN-THE-MIDDLE

En hacker har fået adgang til at læse, ændre eller stjæle oplysninger, der bliver sendt mellem to enheder i din virksomhed.

**Tab ved angreb**
Din virksomhed taber 15 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## SQL INJECTION

En hacker har anvendt skadelig kode på din virksomheds hjemmeside og hentet oplysninger om dine kunders kreditkort.

**Tab ved angreb**
Din virksomhed taber 20 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## ZERO-DAY EXPLOIT

**Alle virksomheder angribes**
Der er en sårbarhed i din virksomheds software. Det bliver udnyttet af hackere, førend du når at opdage og rette det.

**Tab ved angreb**
Din virksomhed taber 20 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## ROOTKIT

Din virksomhed er udsat for et angreb, hvor skjult software giver hackerne kontrol over virksomhedens it-system.

**Tab ved angreb**
Din virksomhed taber 20 aktiekurspoint

**Bonus ved vellykket forsvar:**
2 Kryptocoins

## CREDENTIAL STUFFING

**Alle virksomheder angribes**
En hacker bruger stjålne brugernavne og adgangskoder fra andre websites til at logge ind på dine systemer.

**Tab ved angreb**
Din virksomhed taber 15 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## EAVESDROPPING

En hacker lytter med på din virksomheds kommunikation, hvilket medfører lækage af fortrolige oplysninger.

**Tab ved angreb**
Din virksomhed taber 20 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## PHISHINGANGREB

**Alle virksomheder angribes**
Dine medarbejdere udsættes for falske e-mails, der prøver at stjæle oplysninger om virksomheden.

**Tab ved angreb**
Din virksomhed taber
20 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## INTERN HACKING

En af dine medarbejdere misbruger sine adgangsrettigheder til at få fat i følsomme data om virksomheden.

**Tab ved angreb**
Din virksomhed taber
30 aktiekurspoint

**Bonus ved vellykket forsvar:**
2 Kryptocoins

## DDoS ANGREB

**Alle virksomheder angribes**
Din virksomheds hjemmeside overbelastes med massiv trafik, så den går ned.

**Tab ved angreb**
Din virksomhed taber 15
aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin


## RANSOMWARE

Hackere inficerer din virksomheds it-systemer med malware, der låser dine filer. Hackerne kræver løsepenge for at frigive filerne.

**Tab ved angreb**
2 kryptocoins

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## KEYLOGGER

Hackere har installeret keyloggere på virksomhedens computere. De kan derfor registrere alt, hvad der bliver tastet på et tastatur. På den måde kan de få fat i adgangskoder og fortrolige data.

**Tab ved angreb**
1 sikkerhedskort

**Bonus ved vellykket forsvar:**
2 Kryptocoins

## BRUTE FORCE

Hackere forsøger at knække dine medarbejderes adgangskoder ved gentagne gæt.

**Tab ved angreb**
Din virksomhed taber 25
aktiekurspoint

**Bonus ved vellykket forsvar:**
2 Kryptocoins

## SOCIAL ENGINEERING

IT-kriminelle forsøger at manipulere dine medarbejdere til at afgive følsomme oplysninger.

**Tab ved angreb**
1 sikkerhedskort

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## MALWARE

**Alle virksomheder angribes**
Hackere indsætter skadeligt software, der er designet til at skade eller hacke din virksomheds it-system.

**Tab ved angreb**
Din virksomhed taber 15
aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## XSS ATTACK

Hackere indsætter ondsindet kode på din virksomheds website for at stjæle kundernes loginoplysninger.

**Tab ved angreb**
Din virksomhed taber
20 aktiekurspoint

**Bonus ved vellykket forsvar:**
2 Kryptocoins

## SPOOFING

En IT-kriminel sender en mail til en medarbejder i din regnskabsafdeling. Den kriminelle udgiver sig for at være direktøren og lokker medarbejderen til at overføre et pengebeløb.

**Tab ved angreb**
Din virksomhed taber
30 aktiekurspoint

**Bonus ved vellykket forsvar:**
2 Kryptocoin

## CLICKJACKING

Brugerne af din virksomheds webshop narres til at klikke på skjulte links og knapper. På den måde får kriminelle adgang til at stjæle data.

**Tab ved angreb**
Din virksomhed taber
15 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

## WATERING HOLE

**Alle virksomheder angribes**
Hackere inficerer websteder, som medarbejdere i din virksomhed ofte besøger. Formålet er at sprede ondsindet software på brugernes computere.

**Tab ved angreb**
Din virksomhed taber 20 aktiekurspoint

**Bonus ved vellykket forsvar:**
1 Kryptocoin

Skal ikke bruges

Skal ikke bruges

Skal ikke bruges

Skal ikke bruges

# KRYPTOCOINS

## AKTIEKURSPOINT

| | | | | |
|---|---|---|---|---|
| 5 | 5 | 5 | 5 | 5 |
| 5 | 5 | 5 | 5 | 5 |
| 5 | 5 | 5 | 5 | 5 |
| 10 | 10 | 10 | 10 | 10 |
| 10 | 10 | 10 | 10 | 10 |
| 10 | 10 | 10 | 10 | 10 |
| 20 | 20 | 20 | 20 | 20 |
| 20 | 20 | 20 | 20 | 20 |
| 20 | 20 | 20 | 20 | 20 |
| 50 | 50 | 50 | 50 | 50 |
| 50 | 50 | 50 | 50 | 50 |