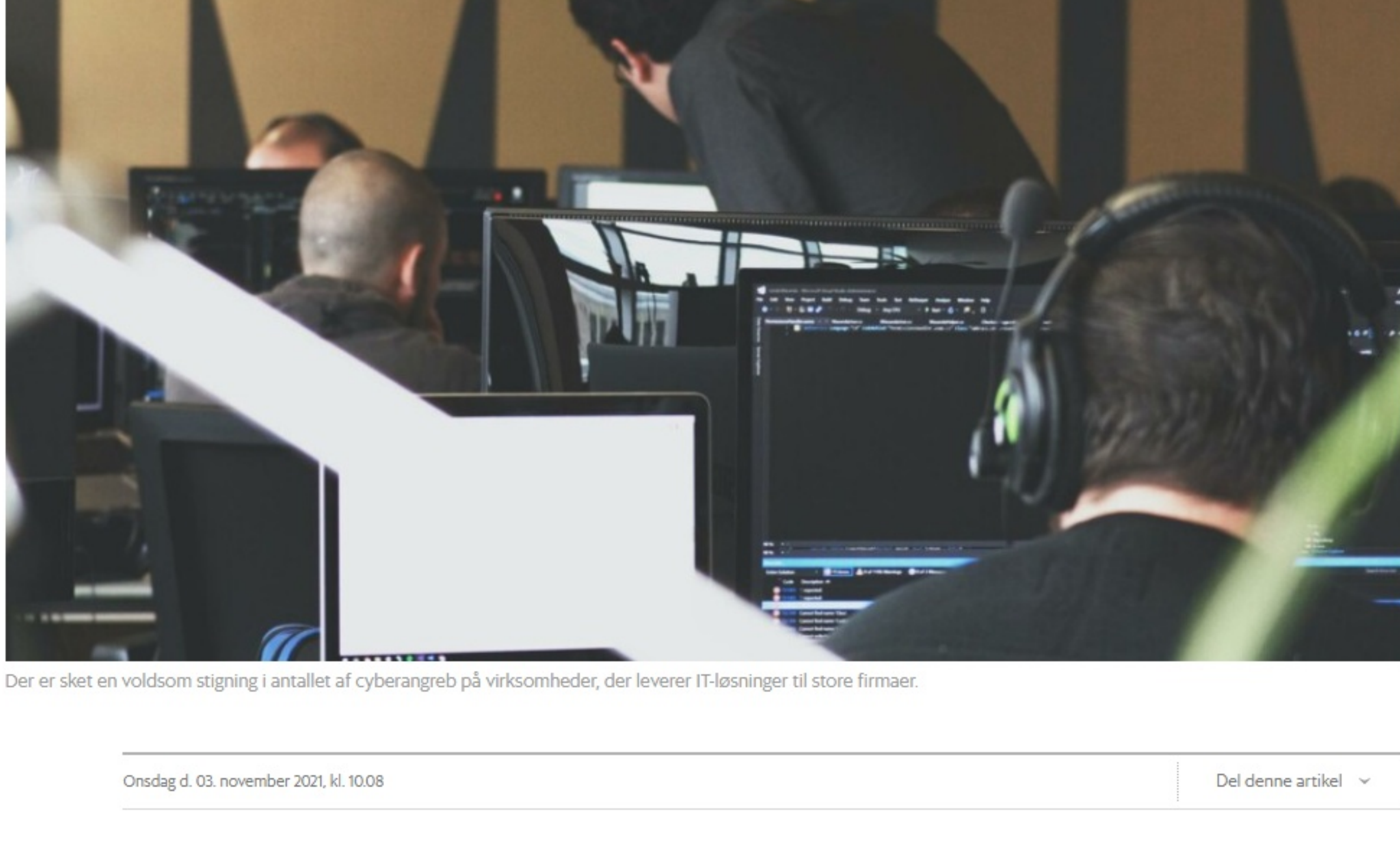


SPONSERET INDHOLD

Cyberkriminalitet i hastig vækst: Sådan beskytter du din virksomhed mod hackerangreb

Truslen fra cyberkriminalitet er rekordhøj i Danmark, og angrebene bliver stadig mere avancerede. Som virksomhed er det vigtigt at være beskyttet så godt som muligt - og ikke mindst være ordentlig forsikret, hvis uheldet er ude.



Der er sket en voldsom stigning i antallet af cyberangreb på virksomheder, der leverer IT-løsninger til store firmaer.

Onsdag d. 03. november 2021, kl. 10:08

Del denne artikel

SPONSERET INDHOLD

I samarbejde med



»Vi ser en ret dramatisk stigning i antallet af cyberangreb for tiden. Det rammer mange forskellige brancher. Der er ikke mindst mange supply chain-angreb mod it-leverandører, der leverer it-løsninger til store virksomheder og myndigheder. Det er absolut noget, man skal tage alvorligt,« siger Maths Stanser, General Manager i QBE Nordics, et af verdens førende forsikringsselskaber og genforsikringsselskaber, der blandt andet tilbyder dækning af forretningsrisiko i forbindelse med cyberangreb.

Center for Cybersikkerhed vurderer, at truslen fra cyberkriminalitet i dag er »meget høj«, og at denne trussel især ligger i de kriminelles evne til konstant at omstille sig til den nye virkelighed i danske virksomheder, myndigheder og borgere. De kriminelle er i stand til lynhurtigt at omstille sig i takt med, at sikkerhedsniveauet i eksempelvis virksomheder udvikles og forandres.



I 2017 blev Maersk ramt af et globalt cyberangreb, som kostede virksomheden et milliardbeløb. Det fik mange andre virksomheder til at stramme op på sikkerheden - og forsikringerne.

Ifølge Maths Stanser skyldes stigningen i cyberkriminalitet dels, at mange medarbejdere har arbejdet hjemmefra gennem de seneste halvandet år. Det er nemlig med til at sænke den generelle sikkerhed.

»Hjemmearbejde er blevet mere udbredt inden for de fleste brancher, og det giver gode muligheder for de kriminelle. De angriber jo mange på samme tid, og der skal bare én åbning til, at de kan komme ind i systemet. Vi ser især mange phishing-angreb, som vi ellers regnede med, ville blive færre med årene. Sådan er det ikke gået, tværtimod.«

Sikkerhed og forsikring

Der er mange forskellige konsekvenser ved et cyberangreb. Mange virksomheder oplever eksempelvis, at de i en periode ganske enkelt mister muligheden for at drive deres forretning, da hele deres forretningsapparatet vil være lagt ned.

»Kan man ikke drive sin forretning, kan man ikke tjene penge, og det kan naturligvis have store konsekvenser for den enkelte virksomhed. Udgifterne forsvinder jo ikke, når forretningen går i stå, så det kan hurtigt blive utrolig dyrt, når store virksomheder som eksempelvis COOP Sverige bliver angrebet. Derfor er det også helt afgørende, at man formår at holde de kriminelle ude,« siger Simon Højmark, Financial Lines Portfolio Manager i QBE.

SIMON HØJMARK, FINANCIAL LINES PORTFOLIO MANAGER, QBE

»Hvad end baggrunden for angrebene er, så er det vigtigste for den enkelte virksomhed at være beskyttet så godt som overhovedet muligt og ikke mindst at være ordentligt forsikret, hvis uheldet alligevel er ude.«

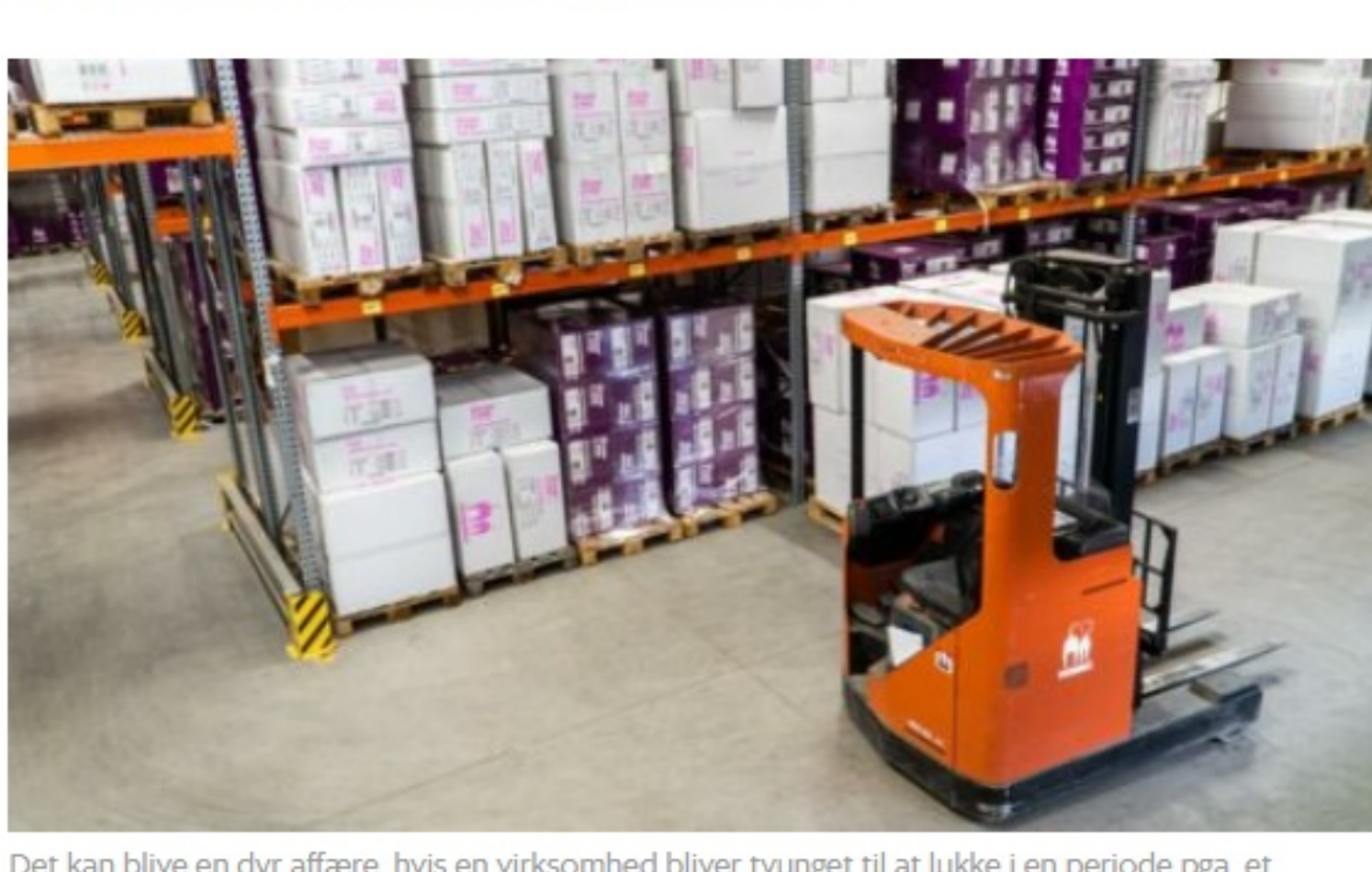
Kriminelles mål for cyberangrebet spænder vidt. Mens nogle er ude efter industrihemmeligheder, går andre efter at stjæle følsomme informationer. Andre igen forlanger løsesummer. Blandt de cyberkriminelle findes formentlig også både stater og efterretningstjenester, men dette er svært at bevise endeligt.

»Hvad end baggrunden for angrebene er, så er det vigtigste for den enkelte virksomhed at være beskyttet så godt som overhovedet muligt og ikke mindst at være ordentligt forsikret, hvis uheldet alligevel er ude. Det er farligt kun at satse på at holde angrebene stangen, for kommer de først indenfor, og man ikke er godt forsikret, kan det blive ekstremt problematisk.«

Vurdering af sikkerheden

En god forsikring mod cyberangreb kan være af afgørende betydning for de virksomheder eller offentlige myndigheder, som er i farezonen for at blive angrebet. Og det kræver også meget af den forsikringsudbyder, man vælger at gå med.

»I QBE arbejder vi benhårdt på altid at være fuldt opdateret med viden om den nyeste udvikling inden for både sikkerhed og i forhold til hvilke angreb, der sker ude på markedet. Det er altafgørende for vores forretning og vores evne til at hjælpe vores kunder, at vi altid er på forkant med udviklingen. Det er derfor, vi er markedsledende på det nordiske marked,« siger Maths Stanser.



Det kan blive en dyr affære, hvis en virksomhed bliver tvunget til at lukke i en periode pga. et cyberangreb.

Selvom QBE ikke kan afværge et angreb, kan man med en forsikring hos QBE få tilbagebetalt noget af den skade, man har lidt som følge af angrebet. Simon Højmark kalder det for en »form for brandforsikring til it-systemer.«

»Vi har et cyber-risk-framework, hvor vi kommer rundt om 15 forskellige områder inden for it-sikkerhed og governance. Her giver vi en vurdering af modenhedsniveauet hos både interne og eksterne leverandører i virksomheder og kan derved hjælpe med at reducere virksomhedens cybersikkerhedsrisiko. Denne metode bliver skræddersyet til den enkelte virksomhed, for der er naturligvis forskel i trusler og behov, hvad enten man er en stor offentlig myndighed eller en lille forsyningsvirksomhed,« siger Simon Højmark.

Arbejdet slutter aldrig

At dæmme op for cyberkriminalitet og ikke mindst at forsikre virksomheder og myndigheder mod de angreb, der finder sted, er også et spørgsmål om konstant at udvikle, ikke bare QBEs, men også erhvervslivets og de offentlige myndigheders viden og forståelse for cyberangreb og de konsekvenser, angrebene kan have.

»Det er mit indtryk, at den generelle viden om cyberkriminalitet er steget markant gennem de seneste år. Det er utrolig godt for alle, der er i risikozonen for at blive angrebet. Førhen var det noget, man talte om i den enkelte it-afdeling, men nu er det også blevet et emne på direktiongangene. Hvert angreb, der finder sted, viser jo tydeligt, hvorfor det er så utrolig vigtigt at kende sine risici som virksomhed og vide, hvordan man forsikrer sig bedst muligt,« siger Maths Stanser.

FAKTA

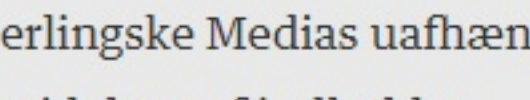
Om QBE - Forsikring

- QBE er ét af verdens førende forsikringsselskaber og genforsikringsselskaber, der tilbyder dækning af forretningsrisiko i forbindelse med blandt andet cyberangreb.
- QBE har arbejdet med kunder i Danmark siden 2006. Virksomheden har et lokalt kontor i Danmark og har specifik viden om danske forhold og lokaler.

FOLD UD

En større forståelse for hvilke risici, man som virksomhed eller myndighed har internt og eksternt, giver ifølge Maths Stanser ikke alene en bedre chance for at undgå angreb fra cyberkriminelle. Det gør det også nemmere at få den bedst mulige forsikring, hvis uheldet skulle være ude.

»Alle vores kunder får en skræddersyet løsning, der tager udgangspunkt i kundens interne setup og naturligvis også i lignende virksomheder og tidligere angreb. I QBE har vi så mange kunder i forskellige brancher, at vi er tvunget til hele tiden at blive klogere og bedre for at kunne fremtidssikre vores virksomhed og gøre en forskel for vores kunder. At dæmme op for cyberangreb er et arbejde, der aldrig slutter,« siger Maths Stanser.



Dette indhold er produceret af Berlingske Media i samarbejde med en annoncør. Berlingske Medias uafhængige redaktioner har intet at gøre med udarbejdelsen af indholdet.

Til forsiden

