Praktijkvoorbeelden cybercriminaliteit

Malware bij advocatenkantoor

Wat is er gebeurd?

Agressieve malware heeft het digitale archief en administratiesysteem van een advocatenkantoor platgelegd. De hacker heeft gebruik gemaakt van verouderde systemen om binnen te komen. Er wordt losgeld gevraagd.

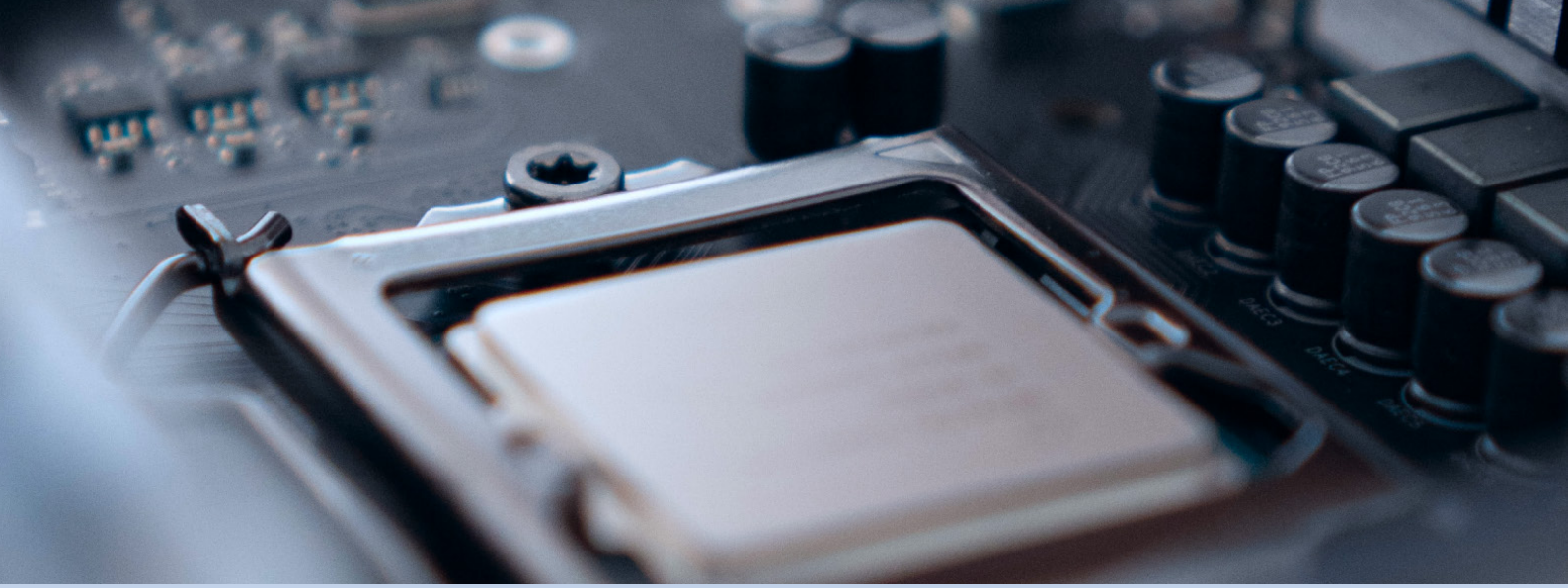
Bijkomend probleem is dat de laatste back-up ook malware bevat. Het kantoor ligt een aantal dagen volledig stil. Het archief en administratiesysteem moet handmatig aangevuld worden. Het bedrijf draait op halve kracht. De omzet loopt evenredig terug.

Kosten incident

€ 170.000

Direct actie ondernemen is van groot belang!

- Een incidentmanager coördineert de noodsituatie
- Een forensisch ICT-bedrijf onderzoekt of er nog back-ups zijn zonder malware en probeert de malware veilig te verwijderen
- Er wordt een onderhandelingsexpert ingezet die de ransomwaresituatie beoordeeld. In het uiterste geval wordt losgeld betaald
- Heeft er een datalek plaatsgevonden? Zo ja, dan moet dit gemeld worden
- Er wordt juridisch advies ingewonnen over de wijze waarop klanten geïnformeerd moeten worden
- De verloren gegevens worden handmatig opnieuw aan het systeem toegevoegd tijdens de gijzeling
- Er wordt een persbericht op website geplaatst
- Afspraken met klanten worden afgezegd
- Het kantoor ligt drie dagen volledig stil en heeft nog twee weken last van ontbrekende gegevens, waardoor afspraken niet door kunnen gaan
- Een ICT-bedrijf onderzoekt hoe toekomstige hacks voorkomen kunnen worden en verbetert de systemen



Webshop wordt slachtoffer van phishing

Wat is er gebeurd?

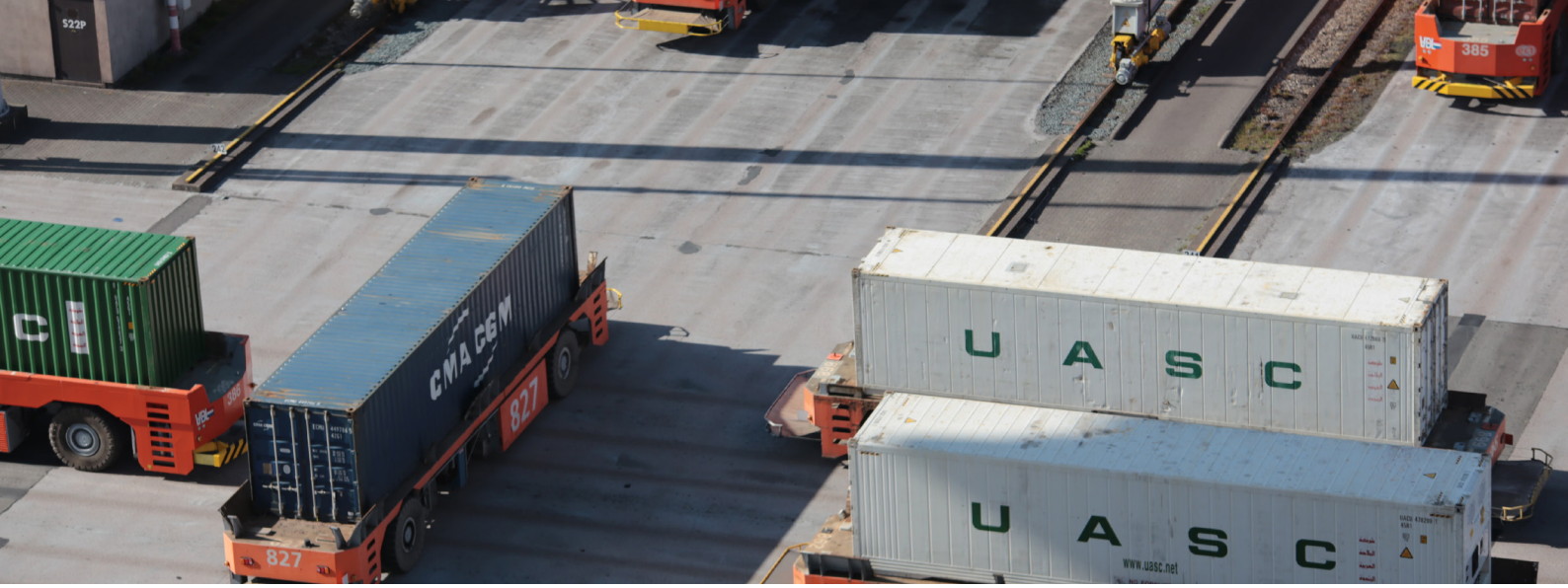
Een medewerker van een webshop heeft op een phishing link geklikt. De hacker heeft nu toegang tot de webshop en persoonsgegevens van klanten. Dit wordt niet opgemerkt tot er bij klanten allerlei creditcardbetalingen worden afgeschreven. Na onderzoek blijkt dat het klantenbestand van de webshop op het dark web is verhandeld. Een groot aantal klantgegevens is gestolen, waaronder creditcardgegevens. Klanten bij wie geld is afgeschreven spreken de webshop hierop aan. Dit incident bereikt het nieuws.

Kosten incident

€ 210.000

Direct actie ondernemen is van groot belang!

- Een incidentmanager coördineert de noodsituatie
- Een forensisch ICT-bedrijf onderzoekt oorzaak en impact hack en sluit toegang af
- Een PR-bureau wordt ingezet om de communicatie te begeleiden
- Een jurist met expertise op gebied van AVG en privacy wordt ingezet om te begeleiden bij claims en boetes van toezichthouders
- Alle mogelijk betrokken klanten worden geïnformeerd
- Rekeningen van deze klanten worden gemonitord op verdachte activiteiten
- Schade van gedupeerde klanten wordt vergoed
- De Autoriteit Persoonsgegevens legt een boete op
- Het datalek wordt gemeld
- Er wordt een persbericht opgesteld
- Voor medewerkers die getroffen klanten te woord staan wordt een Q&A opgesteld
- Medewerkers krijgen een training om toekomstige incidenten te voorkomen



CEO fraude bij transportbedrijf

Wat is er gebeurd?

Een financieel medewerker maakt € 15.000 over naar een cybercrimineel die zich, na uitgebreid vooronderzoek, voordoet als de algemeen directeur. Enkele dagen later wordt ontdekt dat dit verzoek niet van de algemeen directeur kwam. Tegen die tijd is het geld alweer van de rekening waar het naartoe is geboekt verdwenen. Na onderzoek blijkt dit rekeningnummer van een geldezel te zijn, die geen idee had dat hij betrokken was bij een misdrijf.

Kosten incident

€ 27.000

Direct actie ondernemen is van groot belang!

- Er wordt onderzocht of het geld terug te halen is
- Er wordt beoordeeld of de cybercrimineel de systemen van het transportbedrijf heeft gehackt. Als dit zo is, dan moet het systeem hersteld worden
- De bank kan de boeking niet meer achterhalen: € 15.000 is verdwenen
- Het personeel krijgt een awareness training
- De processen worden opnieuw beoordeeld

Hienfeld