Joey Fennis, hoofd van het team Computer Emergency Response Team

“Wij opereren vaak als de **digitale brandweer**”

Joey Fennis is hoofd van het team Computer Emergency Response Team van DataExpert te Veenendaal. Met zijn tienkoppige team is hij full time bezig met preventie en bestrijding van (geavanceerde) cyberaanvallen.

We interviewen regelmatig collega’s die veel met data en informatie werken, ervaringen hebben op dit gebied en ons nuttige inzichten kunnen bieden. Dit doen we vanwege ontwikkelingen binnen de Rijksoverheid, die meer van ons gaan vragen dan de afgelopen jaren het geval was. Voor dit artikel stelden we vragen aan een externe expert. Volg de groep Goed omgaan met overheidsinformatie op Plek voor meer informatie! Deel 13.

Dagelijks wordt Joey geconfronteerd met de gevolgen van cybercriminaliteit. In dit interview vertelt hij onder meer hoe cybercriminelen te werk gaan.

Reactieve en proactieve hulp

Bedrijven schakelen DataExpert in bij diefstal van data of een cyberaanval. “Wij opereren vaak als de digitale brandweer”, vertelt Joey. “Veel bedrijven denken dat wij met het toverstafje zwaaien en hun probleem is opgelost. Helaas duurt het altijd even voor we inzicht hebben in een voor ons nieuw bedrijfsnetwerk. Bovendien heerst er chaos bij het management, de directie en de ict’ers. Wat wij vaak tegenkomen, is ransomware. Dan hebben aanvallers bestanden gestolen, versleuteld of gegijzeld en dreigen ze bijvoorbeeld om vertrouwelijke data op het darkweb te publiceren als er geen losgeld wordt betaald. Daarmee zetten ze een bedrijf onder druk om te betalen om de toegang tot hun gegevens terug te krijgen. We adviseren organisaties ook proactief, door ervoor te zorgen dat zij kwaadwillenden eerder in hun netwerk kunnen detecteren en elimineren.”

Ransomwareketen

Bij een cyberaanval werken verschillende specialismen samen in een professioneel opgezette ‘ransomwareketen’. Joey: “Initial access brokers (tussenpersonen) onderzoeken hoe ze een bedrijf kunnen binnenkomen, bijvoorbeeld via gestolen inloggegevens of een kwetsbaarheid op een server. Die informatie verkopen ze aan hackers, die vervolgens het netwerk binnendringen. Hackers zoeken naar vertrouwelijke data om te stelen, verwijderen de back-ups en zetten als laatste zoveel mogelijk bestanden op slot met door developers ontwikkelde ransomware. Een datamanager beheert vervolgens de gestolen data en stuurt deze naar een server van een bulletproof hosting partij (een bedrijf dat moedwillig criminele klanten werft en verdient aan het faciliteren van hun illegale activiteiten). Wanneer het slachtoffer aangeeft te willen betalen, helpt de customer care, de onderhandelaars, het bedrijf door het betaalproces heen. Wil een bedrijf niet betalen, dan zetten ‘chasers’, de digitale knokploeg, het MT of de Raad van Bestuur via appjes of mails onder druk met de mededeling dat ze hun data hebben en dat ze moeten betalen, hoe je dat moet doen en wat er gebeurt als je niet betaalt.”

> “Aanvallers bouwen achterdeurtjes in, zodat ze bij een herstart of terugzetten van back-ups opnieuw connectie hebben met de omgeving van het slachtoffer”

Waarom aanvallen?

“Cybercriminelen hebben verschillende motieven om bedrijven aan te vallen”, weet Joey. “De georganiseerde criminaliteit doet het vaak voor financieel gewin. ‘Hacktivisten’ vallen aan omdat ze een politiek of maatschappelijk doel willen bereiken. Een actueel praktijkvoorbeeld van ‘statelijke actoren’ is dat Russische hackers in opdracht van de overheid malware ontwikkelen om de vitale infrastructuur in de Oekraïne plat te kunnen leggen. Of Chinese hackers die Europese bedrijven aanvallen om intellectueel eigendom te stelen. Bij bedrijven in de maak- en productie-industrie kan een aanvaller de bestanden op slot zetten, waardoor een fabriek niet meer kan produceren. Zorginstellingen, ziekenhuizen en scholengemeenschappen zijn heel bang dat hun medische, medewerkers- of leerlingendossiers op straat komen te liggen. Bij ziekenhuizen kan het gevolg van een aanval zijn dat zorg of operaties niet kunnen doorgaan.”

En als je niet betaalt …

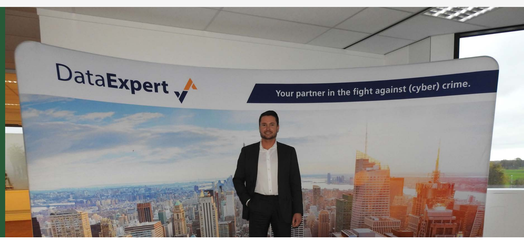
“Betaal je niet en staan je gegevens op het darkweb, dan kunnen kwaadwillenden bijvoorbeeld identiteitsfraude plegen met gestolen kopieën van paspoorten. Als wij hebben ontdekt welke data er zijn gestolen, dan kunnen we medewerkers hierover informeren en ze adviseren wat ze moeten doen. Hun paspoort laten blokkeren bijvoorbeeld. Bij een hack worden vaak ook data over het bedrijfsnetwerk van het slachtoffer gestolen. Met deze voorkennis kunnen cybercriminelen nieuwe aanvallen plegen. In principe kan iedereen bij gestolen data op het darkweb. Het is voor bedrijven een angstig idee niet te weten wat ermee gebeurt. We werken voor een scholengemeenschap, die ook bijzonder onderwijs geeft. Je wilt echt niet dat gegevens van die jonge kwetsbare kinderen op straat komen te liggen.”

Orde in de chaos creëren

“Als we bij een bedrijf komen, creëren we eerst orde in de chaos. We gidsen het slachtoffer door het incident heen. Met de mensen van het CMT met onder andere Communicatie, HR en ICT stellen we een ‘warroom’ op. We zetten specialisten bij elkaar die zaken moeten uitzoeken en de warroom daarover informeren en adviseren. In het algemeen worden eerst de interne medewerkers geïnformeerd over een incident. Zijn we wat verder in het onderzoek, dan kunnen ook klanten, leveranciers en andere stakeholders worden ingelicht. Als er ook data van klanten zijn gestolen, dan moeten zij daarover worden geïnformeerd. En we moeten het datalek melden bij de Autoriteit persoonsgegevens.

We proberen de klant zo snel mogelijk en op een veilige manier terug te brengen naar normaal. Daarvoor moeten we uitzoeken wanneer en hoe de aanvallers binnen zijn geweest en wat ze in een netwerk hebben gedaan. Met die informatie kunnen we nadenken hoe we het bedrijf weer gesegmenteerd online kunnen brengen. Om dat veilig te kunnen doen, proberen we van de aanvaller een soort profiel op te bouwen. Want aanvallers bouwen achterdeurtjes in, zodat ze bij een herstart of terugzetten van back-ups opnieuw connectie hebben met de omgeving van het slachtoffer. Tijdens een cyberincident stellen we vaak een ‘verhoogde dijkbewaking’ in, waarbij we met onze software alle systemen in het netwerk van de klant monitoren. Als we dan iets terugbrengen in productie, zien we het direct wanneer er gekke dingen gebeuren en kunnen we dat direct elimineren of uitzetten. Als we klaar zijn, laten we die verhoogde dijkbewaking vaak preventief nog een aantal maanden aanstaan.”

> “Betaal je niet en staan je gegevens op het darkweb, dan kunnen kwaadwillenden bijvoorbeeld identiteitsfraude plegen met gestolen kopieën van paspoorten”



Politie en samenwerking

DataExpert heeft goede contacten met de politie. Joey: “Er werken bij ons veel oud politiemensen. Daardoor kunnen we samen met het slachtoffer meteen bij de juiste regio en digitale experts aangifte doen. We delen de technische details van aanvallen met de politie. Zo kunnen we samen cybercriminaliteit tegengaan of remmen en inzicht geven in de omvang van en ontwikkelingen in cybercriminaliteit.

Samen met andere grote incident response partijen zitten we in een samenwerkingsverband met het Openbaar Ministerie, de politie, het Nationaal Cyber Security Centrum en Cyberveilig Nederland. Hierin delen we kennis over hoe criminelen binnenkomen, wat ze stelen, hoeveel schade dat veroorzaakt, hoeveel mensen er betalen, hoeveel losgeld er wordt geëist en over de achtergrond van een aanvallerscollectief. Zo bundelen we de krachten om Nederland meer cyberweerbaar te maken.”

Februari 2024