

FRAUDE Gegevens zijn wel aanwezig, maar worden te kort en niet in een makkelijk doorzoekbare vorm bewaard

Bedrijven zijn niet klaar voor forensisch onderzoek

■ Organisaties richten zich op compliancy en back-up

■ Beveiliging te veel op externe gevaren gericht

Weinig organisaties beschikken over de juiste gegevens die nodig zijn om fraudeonderzoek beter mogelijk te maken. Naïviteit en onwetendheid zijn hiervan de belangrijkste oorzaken. “Organisaties richten zich vooral op compliancy en back-ups. Alleen daarmee ben je echter niet in control”, zegt Mark Hoekstra, medeoprichter van IRS Forensic Services & Investigations in Rotterdam. “Als er iets fout gaat in de organisatie door malversaties, dan moet je als organisatie wel over de juiste gegevens beschikken om uit te kunnen zoeken hoe en waarom iets fout is gegaan en om te bepalen hoe je voorkomt dat het opnieuw gebeurt.” Hoekstra vindt dat er in de IT veelal verkeerd beveiligd wordt: alleen tegen gevaren van buitenaf. Terwijl al jaren bekend is dat op zijn minst de helft van de problemen van binnenuit komt. “Organisaties negeren dat.”

IRS specialiseert zich onder meer in forensisch IT-onderzoek en IT-beveiliging. Het bedrijf stelt daarbij onder meer gegevens veilig op een forensisch verantwoorde wijze. Ook bewerkt het gegevens zodanig dat ze doorzoekbaar worden. Drie terabyte aan mail is bijvoorbeeld menselijkerwijs niet meer door te lezen. Met behulp van technieken als datamining en taaltechnologie en andere tools kan snel door deze brij van gegevens worden gezocht.

Hoekstra constateert echter dat maar weinig organisaties ‘forensic ready’ zijn. “Dat ben je als je als organisatie klaar bent voor onderzoek aan zowel de organisatorische als de IT-kant. Je moet je organisatie zo hebben ingericht dat misstanden nagezocht kunnen worden. Wordt er bijvoorbeeld informatie gelekt, dan heb je de juiste gegevens opgeslagen om uit te zoeken wie dat heeft gedaan. In de praktijk zien we echter dat nagenoeg alle bedrijven niet ‘forensic ready’ zijn. En dan kost het veel geld om gegevens beschikbaar te krijgen.”

Hij geeft een voorbeeld: “Binnen een multinational is informatie gelekt die invloed heeft op het verloop van de koersen. De gegevens die nodig zijn voor het forensisch onderzoek, zijn bijvoorbeeld:

- Telefoongegevens.
- Mobieletelefoongegevens. Die zijn voorhanden bij de provider, maar vaak krijg je alleen via de rekening de gegevens over uitgaande gesprekken. Die moeten bovendien doorzoekbaar gemaakt worden.
- Gegevens van de interne communicatie: regulier mailverkeer, maar ook webmail, chatverkeer, Skype.
- Vergaderverslagen – hierin wordt vastgelegd waar welke kennis zit.
- Open-bronnenonderzoek zoals kranten en tijdschriften. Er is bijvoorbeeld iets gelekt naar een grote krant. Dan kijk je wat die krant het afgelopen jaar over die organisatie heeft gepubliceerd. Dan ga je vaak al patronen zien. Combineer je dat met telefoongegevens, dan is de kans al heel groot dat je ziet wie gelekt heeft.
- Gebruik van pc’s.

■ Gegevens van aanwezigheidsregistratie: Wie was wanneer waar?

■ Contactpersonen die staan opgeslagen in telefoons, outlook, belhistorie, etc. Gebruik je al die bronnen, dan is er een redelijke kans dat je de daders vindt”, zegt Hoekstra.

Als bestuurder moet je eens met de Forensic Readiness-blik naar je organisatie kijken. Het zijn echt geen gigantische trajecten. Veel gegevens die nodig zijn, zijn al aanwezig in de organisatie, maar ze worden vaak te kort bewaard of zijn moeilijk doorzoekbaar. Neem bijvoorbeeld de loggegevens van financiële bestanden. Vaak zijn die opgeslagen op plaatsen waar men niet bij kan. Of ze worden verkeerd bewerkt, waardoor ze verloren gaan. Meestal vereist het maar een kleine ingreep om die gegevens wél op de juiste manier te bewaren.

Neem de logs van een webserver. De gegevens van bezoek aan jouw websites worden standaard gelogd. Die logs zijn echter vaak verdeeld over een aantal servers. Ze zijn meestal niet uniform, doordat de data bijvoorbeeld in een andere volgorde worden opgeslagen. Het is achteraf heel veel werk om die gegevens te uniformeren. Doe je dat vooraf, dan scheelt dat heel veel onderzoekskosten.

Bedenk wel dat een groot onderzoek al snel tonnen kost.”

Volgens Hoekstra beseffen maar weinig bedrijven dat ze dat heel veel geld kan schelen. “Het is soms een vorm van naïviteit. Maar vaak maakt men ook een afweging als er besloten moet worden om een onderzoek te doen: Wat is de kans dat het succes oplevert en wat krijg je er dan voor terug? Dat zou echt niet de enige reden mogen zijn. Je moet ook in control zijn. Je moet willen weten hoe je vijf ton bent kwijtgeraakt. Vaak heeft een bedrijf wel enig idee hoe dat gebeurd is, maar niet precies. Weet je het wel precies, dan kan een eenvoudige maatregel al afdoende zijn om het een volgende keer te voorkomen.”

Misstanden in een geautomatiseerde omgeving komen vaak voort uit onvrede bij

IT'ers, constateert Hoekstra. Die onvrede groeit omdat ze zich niet erkend voelen. “IT'ers hebben vaak een enigszins anarchistische inslag. De geautomatiseerde omgeving is hun kindje. Als het management dan besluit bepaalde dingen niet te doen, voelt een IT'er zich miskend. Dat gevoel kan gemeengoed worden als je die cultuur laat bestaan. Die onvrede uit zich dan in kwajongensstreken, maar dat kan ook uitmonden in het stiekem inbouwen van achterdeuren in de beveiliging van de infrastructuur. Dan wordt het levensgevaarlijk voor een organisatie. Bedrijven blijven echter volhouden dat ze zich daar geen zorgen over hoeven te maken omdat het bij hen niet zou gebeuren. Maar bedenk dan wel dat wij leven van bedrijven waar het wél gebeurt. En we groeien heel hard.”

Hoekstra adviseert bedrijven in elk geval zelf een audit te doen op ‘forensic readiness’, of dat te laten doen. “Alleen al het opstellen van een procedure voor wie wat moet doen bij onderzoek zou helpen. En dat is bepaald geen ‘rocket science’.”

Tanja de Vrede/t.vrede@sdu.nl