Bent u al 'Forensic Ready'?

INZICHT IN UW DIGITALE VEILIGHEID

Secura heeft meer dan twee decennia ervaring in informatiebeveiliging en privacy op het gebied van mensen, processen, techniek en organisatie. Wij identificeren IT-beveiligingsrisico's vanuit een onafhankelijk standpunt, waarbij het hoogste niveau van vertrouwelijkheid en integriteit behouden blijft. Dit stelt u in staat om proactief de controle te houden over de eigen digitale veiligheid.

Het Forensic Readiness Maturity Model

Vrijwel alle organisaties zijn tegenwoordig afhankelijk van informatietechnologie (IT). Naast IT op kantoor is thuiswerken niet meer weg te denken uit onze maatschappij. We gebruiken ook steeds meer Internet-of-Things (IoT) apparaten. Door deze ontwikkelingen ontstaan steeds meer potentieel kwetsbare systemen die vaak ook nog met elkaar in verbinding staan en daardoor nieuwe risico's met zich mee brengen. Net als in de fysieke wereld is het belangrijk deze digitale wereld te beschermen tegen ongeoorloofd gebruik en maatregelen te nemen om vast te kunnen stellen wat er bij een bepaald systeem gebeurd is. Digitaal forensisch onderzoek is het vakgebied dat zich bezighoudt met het opsporen en traceren van incidenten in digitale systemen.

Digitaal onderzoek is essentieel om te kunnen leren van incidenten die zich hebben voorgedaan en incidenten in de toekomst te voorkomen. Gebruikers van informatiesystemen laten namelijk digitale voetafdrukken achter wanneer ze de systemen gebruiken - of het nu gaat om computersystemen, smartphones, mobiele telefoons, tablets of netwerken. Er zijn digitale forensische tools en technieken beschikbaar voor het ophalen en analyseren van digitaal bewijsmateriaal. Digitale forensische tools en technieken kunnen ook worden gebruikt om bijvoorbeeld verloren bestanden te herstellen of om interne systemen te monitoren.

Een incident kan ook leiden tot bijvoorbeeld verzekeringsclaims of de noodzaak tot een juridische afhandeling. Er moet dan achterhaald kunnen worden wie verantwoordelijk is voor het incident (bijvoorbeeld een externe partij of interne medewerker) en wat de reden van het incident is (onwetendheid, nalatigheid, kwaadwillende opzet, fraude of sabotage, en dergelijke). In dat geval moet het digitale onderzoek aan regels voldoen om het resultaat later juridisch te kunnen gebruiken.

Forensisch onderzoek wordt steeds belangrijker

Digitaal forensisch onderzoek is een vakgebied dat nog in ontwikkeling is. Het kan worden gedefinieerd als het gebruik van computer- en informatiesystemen (IS) -kennis, in combinatie met juridische kennis, om op een juridisch aanvaardbare manier digitaal bewijsmateriaal dat is verkregen, verwerkt en opgeslagen op een wettelijk aanvaardbare manier te analyseren.

Digitaal forensisch onderzoek wordt voornamelijk gebruikt voor onderzoeken die zijn gericht op juridische of wetshandhavingskwesties die waarschijnlijk voor de rechter zullen eindigen; vandaar de nadruk op juridische aanvaardbaarheid. Digitaal bewijs is uiterst vluchtig en kan gemakkelijk verloren gaan of worden aangepast. Het is dus nodig om digitaal bewijsmateriaal te bewaren en te behandelen op een manier die ervoor zorgt dat het niet wordt vervormd of vernietigd, en ook niet lijkt te zijn vernietigd.

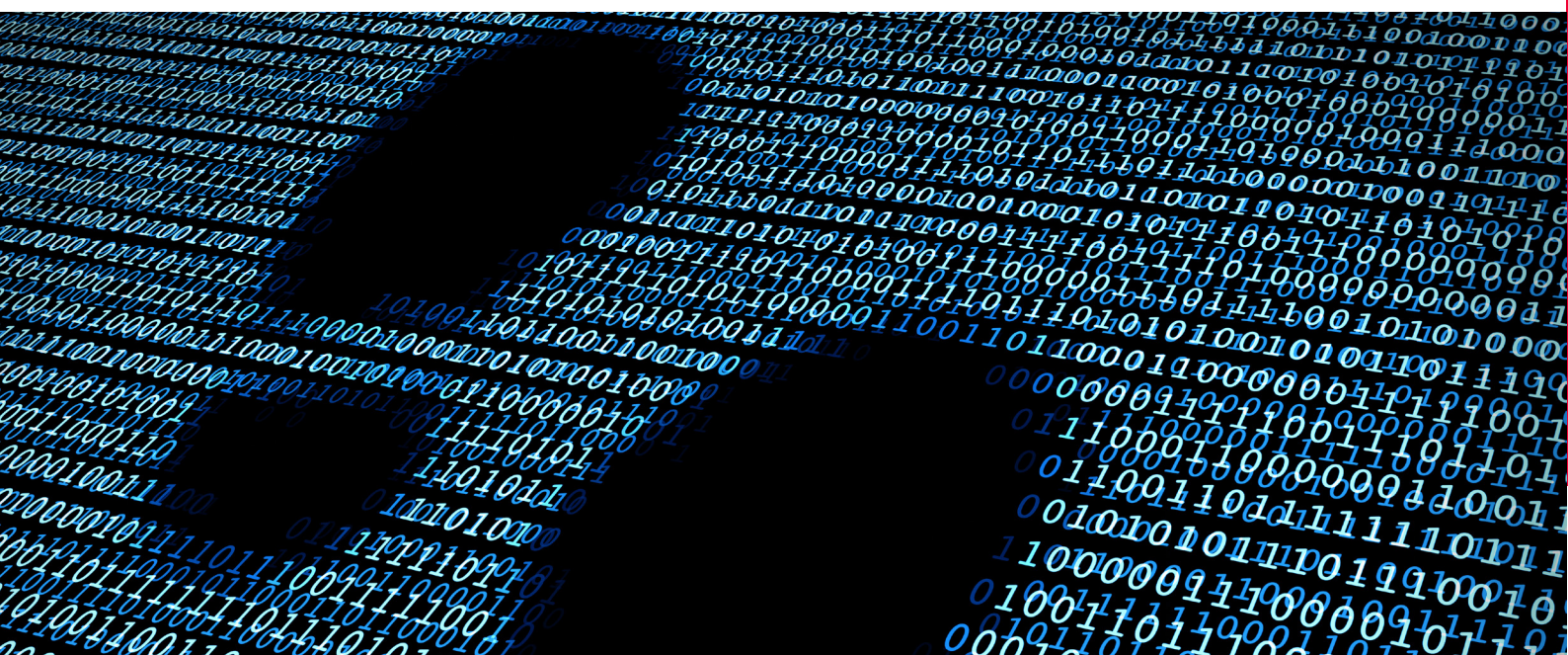
Forensic Readiness

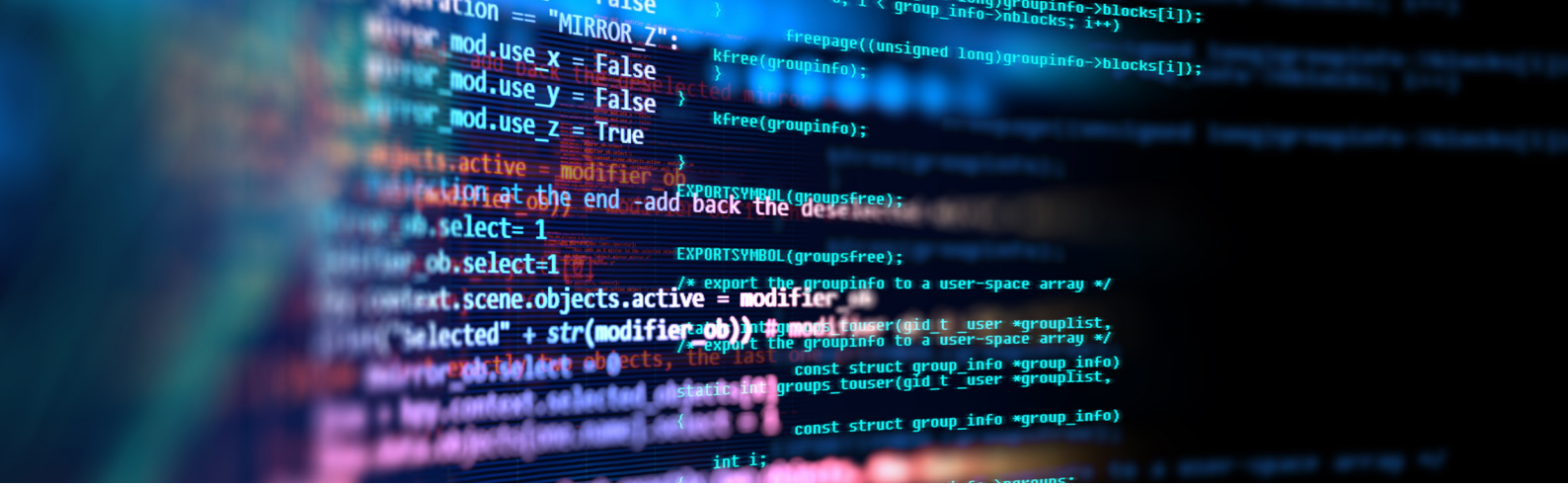
Forensic Readiness geeft aan in hoeverre een organisatie in staat is digitaal bewijs te verzamelen, bewaren, beschermen en analyseren zodat het effectief gebruikt kan worden bij beveiligingsonderzoeken, beantwoording van regelgevende instanties, interne juridische kwesties of in de rechtszaal. Forensic Readiness is een doorlopend proces: met veranderingen in de infrastructuur of het risicoprofiel moet ook de Forensic Readiness opnieuw beoordeeld worden.

Waarom is Forensic Readiness nodig?

Organisaties hebben vaak een incident-response programma, trainingen om hun medewerkers bewust te maken van IT-risico's en bedrijfscontinuïteitsplannen met als belangrijkste doel de incidenten goed en snel af te handelen en in de toekomst te voorkomen.

Forensic Readiness vult hierop aan en zorgt via beleid, implementatie van dat beleid en het valideren van de implementatie om zo goed mogelijk voorbereid te zijn als een incident heeft plaatsgevonden. Het beleid vormt dan de leidraad tijdens de afwikkeling van incidenten Het doel is om zoveel mogelijk bewijsmateriaal veilig te stellen terwijl de kosten en tijdinvestering daarbij minimaal zijn. Het afhandelen van incidenten is vaak tijd-kritisch; zonder een gevalideerd plan waarbij de relevante interne stakeholders en externe partijen vooraf bekend zijn zal kostbare tijd, en wellicht bewijs, verloren gaan.





Belang voor organisaties

Steeds meer organisaties gebruiken data in de 'Cloud' door middel van Office 365. Vrijwel alle commerciële bedrijven en overheden met een website zijn kwetsbaar voor aanvallen via het web. Dat blijkt ook wel uit de dagelijkse meldingen van nieuwe aanvallen.

Vanuit AVG is het belangrijk om te weten over welke data jouw organisatie beschikt om deze te beschermen. De meldplicht datalekken verplicht iedere organisaties een ernstig datalek direct te melden bij de Autoriteit Persoonsgegevens. Maar dan moet je wel weten of en welke data er mogelijk gestolen zijn.

Als een organisatie zich gedegen voorbereidt door middel van Forensic Readiness, dan kent niet alleen de CISO het beveiligingsbeleid, maar weten álle verantwoordelijken hoe ze moeten handelen.

Chain of Custody

Chain of custody (CoC) is vereist om de zekerheid te bieden dat digitaal bewijsmateriaal met de nodige zorg is verzameld, verwerkt, behandeld en opgeslagen, zodat het niet wordt gewijzigd of vernietigd, of dat dit niet kan worden afgeleid. Chain of custody omvat documentatie van hoe digitaal bewijsmateriaal wordt verkregen, verwerkt, behandeld, opgeslagen en beschermd, en wie het bewijs heeft behandeld en waarom - vanaf het punt van verzameling tot het presenteren als een bewijsstuk (bijv. In de rechtbank of op een zitting van een raad van bestuur).

Forensic Readiness Model

Steeds meer organisaties hebben een vorm van een Forensic Readiness plan. Zo'n plan moet meebewegen en actueel zijn en dus regelmatig geëvalueerd worden. Ook moet het beleid bekend zijn binnen de hele organisatie: als er bijvoorbeeld een malware incident is moet je dan je computer aan laten om bewijsmateriaal te bewaren, of uitzetten om de risico's op verspreiding te beperken? Vervolgens moet de implementatie regelmatig gevalideerd worden door incidenten te simuleren. Met een Forensic Readiness Maturity meting wordt de volwassenheid van een organisatie op al deze gebieden meetbaar gemaakt. Het is daarmee een geweldige manier om objectief te bepalen wat het maturity niveau is en waar verbeteringen het meest effectief zijn. Ook kunnen zo risico's van het ontbreken van bepaalde maatregelen meetbaar in kaart gebracht worden.

Voordelen van Forensic Readiness

- Een organisatie heeft een **voorsprong** bij het afhandelen van een incident. Met een duidelijk plan kan er sneller bewijs worden verzameld en geanalyseerd waardoor de impact van een incident verkleind wordt.
- Het wordt **gemakkelijker en goedkoper** om digitale bewijslast te verzamelen. De benodigde data is daardoor beschikbaar en het bewijs gemakkelijker en goedkoper te overleggen.
- Er gaat een preventieve werking uit van een **grotere pakkans**. Het wordt een interne medewerker of externe hacker moeilijker gemaakt om ongezien weg te komen.
- Het beleid en verbeteringen daarop worden **meetbaar** gemaakt.
- Met Forensic Readiness geeft een organisatie blijk dat **het informatiebeveiligingsbeleid op orde is.**

Secura
A BUREAU VERITAS COMPANY

Hoe helpt Secura uw organisatie Forensic Ready te worden en te blijven?

Wellicht is uw organisatie al in hoge mate 'Forensic Ready' en wilt u dit meetbaar maken. Of uw organisatie heeft als doel de eerste stappen te nemen, maar het is onduidelijk welke stap het meeste resultaat sorteert. Secura heeft een Forensic Maturity Model ontwikkeld dat op alle kritische aspecten van Forensic Readiness aan de hand van interviewvragen zowel een overall score, als een score op elk onderdeel geeft. Secura kan u helpen met een nulmeting om uw huidige Forensic Readiness vast te stellen en aan de hand daarvan te bepalen welke vervolgstappen het meest efficiënt zijn voor uw organisatie.

Secura: uw partner bij forensisch onderzoek

Ondanks de beveiliging van IT-systemen komen security-incidenten dagelijks voor. Secura is een geregistreerd particulier onderzoeksbureau en wij hebben 'particulier onderzoekers' in dienst die digitaal forensisch onderzoek mogen doen en op rechtsgeldige manier bewijsmateriaal verzamelen. Deze dienst leveren wij voor al onze klanten die te maken hebben gehad met een security-incident. Uiteraard is ons onderzoek het meest effectief en efficiënt als de organisatie waar wij het onderzoek doen al 'Forensic Ready' is.

Heeft u interesse in het uitvoeren van een digitaal forensisch onderzoek of heeft u vragen over wat wij hierin kunnen betekenen voor u? Neem dan contact op via info@secura.com.

Wij helpen u graag verder!

Secura
A BUREAU VERITAS COMPANY

Interesse?

Neem contact op met ons:

Volg ons op:

+31 88 888 31 00
info@secura.com
secura.com

BUREAU VERITAS
1828
BUREAU VERITAS
Shaping a World of Trust