

Computer-forensics

Computer Forensics is het gebruik van wetenschappelijk bewezen methodes voor het samenbrengen en verwerken van gegevens aangetroffen op een digitaal toestel (computer, harde schijf, GSM, geheugenkaart, enz.) en het interpreteren van die gegevens voor mogelijk gebruik in een rechtbank of onderzoek. Het bewijsmateriaal kan dienst doen bij het vervolgen van een misdadiger, het verdedigen van een beschuldigde of kan iemand helpen die kennis zoekt omwille van persoonlijke of professionele redenen.

De voornaamste gebruikers van Computer Forensics zijn wetsambtenaren, vermits een groot percentage van misdaden op een zekere manier gebruik maken van digitaal opgeslagen gegevens. Die gegevens omvatten een telefoongesprek met een GSM, waardoor een individu op de plaats delict geplaatst kan worden (of net niet natuurlijk), sporen van illegale activiteiten zoals drughandel, pedofiele afbeeldingen, human resource-kwesties, hacking, e-mailmisbruik, niet-toegestaan reproduceren van gegevens, IP-diefstal, enz. Bedrijfsorganisaties gebruiken steeds meer computer forensics vermits ze vaak voorvallen moeten onderzoeken zoals ongepast computergebruik, ongepast e-mailgebruik, niet-toegestaan reproduceren van gegevens en bedrieglijke werknemers. Human Resource-afdelingen en interne veiligheid zijn de grootste gebruikers van deze gespecialiseerde bedrijfsdiensten. Ook privé-personen kunnen deze diensten gebruiken. Dat kan gaan van iemand die zijn partner bedriegt tot ongepast internet-gebruik door een gezinslid.

Computer Forensics onderzoek

De 4 belangrijkste stappen van het forensisch onderzoek op computer:

1. Naleven richtlijnen voor de recuperatie van digitaal bewijsmateriaal, met een uitgebreid controleerbaar proces

2. Behoud het bewijsmateriaal

Gegevens opgeslagen op een computer kunnen vernietigd worden of gemakkelijk ontoegankelijk gemaakt worden. De belangrijkste opdracht is om de juiste procedures te gebruiken om bij de gegevens te geraken. Belangrijk bewijsmateriaal kan zich bevinden in gewiste bestanden of fragmenten van vorige bestanden. Zelfs het inschakelen van de computer kan tot permanent verlies ervan leiden.

3. Werk nooit op de originele media

Eens vastgesteld werd dat de computer of het toestel mogelijk bewijsmateriaal kan bevatten, moet een forensisch beeld gevormd worden voor het onderzoek. Gespecialiseerde hulpmiddelen en software worden gebruikt om wettelijk erkende exacte kopieën te maken van de media voor analysedoeleinden. Deze kopieën zijn niet dezelfde als een normale back-up. Ze bevatten een exacte en forensisch degelijke kopie van elke BIT op de schijf of het toestel.

4. Onderzoeken moeten herhaalbaar zijn.

Computer Forensics is een exacte wetenschap. Men is bezig met bewijsmateriaal, niet met speculeren. De mensenrechten, internationale wetten en de protocollen van de ACPO, NHTCU, zorgen ervoor dat het verzamelen van bewijsmateriaal verloopt volgens internationaal goedgekeurde methodes en dat het gepresenteerd wordt op een manier die goedgekeurd wordt door de rechtbank. Ook expert-getuigen mogen gebruikt worden.

Of het nu gaat om het bestraffen van personeel voor misbruik of het reageren op een dreiging van buitenaf, uw organisatie moet steeds meer omgaan met kwesties die gepaard gaan met het bekijken en recupereren van bewijs uit computers, GSM's, netwerken en andere toestellen.

Bestaande beleidslijnen en procedures kunnen voldoen om de meer traditionele kwesties van wangedrag aan te pakken maar zijn ze ook voldoende voor de nieuwe risico's en kansen veroorzaakt door de steeds veranderende technologie?

De procedures die u hanteert om dreigingen met betrekking tot informatiesystemen aan te pakken kunnen voldoen maar zijn ze ook forensisch gezien uitgebreid genoeg? Zorgen ze ervoor dat u het bewijsmateriaal snel en zonder risico in handen krijgt? Voldoen ze aan de gepaste computer forensics-procedures?

[CARCUR Computer & Digital Forensics Conference zal uw vragen beantwoorden](#)
[November 18-19 2009 World Trade Center Curacao](#)

Bezoek de volgende website voor meer informatie en voor registratie

<http://www.nataxe-logistics.com/forensics.html>