Myndigheten för samhällsskydd och beredskap

FAKTA

Publ.nr: MSB1345 – januari 2019

AVDELNINGEN FÖR CYBERSÄKERHET

OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

IT-forensik i industriella informations- och styrsystem (ICS)

Balansen mellan snabb återställning och IT-forensiska behov vid hantering av intrång för ICS väger för närvarande över till den systemåterställande verksamhetens fördel, vilket leder till att bevis inte alltid tas om hand på korrekt sätt. Den här skriften syftar därför till att ge läsaren grundkunskap för att själv kunna planera för och hantera IT-forensiska händelser i de egna systemen.

Inom all forensisk verksamhet är det grundläggande konceptet att ta vara på och analysera teknisk bevisning på ett sätt så att beviskedjan inte bryts. Det innebär att all hantering ska bevara beviset i ett så opåverkat skick som möjligt och att den eventuella påverkan som sker ska vara känd och spårbar. En mycket viktig princip inom forensiken är att all kontakt lämnar spår.

De tre grundpelarna (aktivitet, resultatvärde och tid)

Grundpelarna ska genomsyra allt IT-forensiskt arbete och även den analys och planering som bör göras i förväg. Till **aktivitet** knyts även en utförare och vid en IT-forensisk utredning är det utföraren av aktiviteten som ska ringas in. Vid egen aktivitet är det viktigt att föra loggbok över vad som gjorts, på vilka data, med vilka verktyg och på vilket sätt. Under grundpelaren **resultatvärde** ryms också kännedom om de verktyg och metoder som används. Verktyg kan innehålla buggar, eller på andra sätt riskera att bryta beviskedjan genom att inte uppfylla de funktionalitetslöften som tillverkaren utställt. Det är därför viktigt att hålla sig uppdaterad om eventuella buggar i verktygen för att kunna ta ställning till hur de påverkar en utredning. Det naturliga sättet att hantera buggar på är att patcha dem, men ur ett forensiskt perspektiv är det sämre än att lämna buggen opatchad och lägga restriktioner på verktygets användning. Vid patchning kan nya okända buggar introduceras och det är bättre ur ett forensiskt perspektiv att känna till brister och hantera dem, än att patcha och på så sätt tappa kunskap om verktygets beteende. Verktygens beteende bör därför i möjligaste mån verifieras genom testning i förväg, för att öka kännedomen om dem. Grundpelaren **tid** handlar främst om tidsstämpling av händelser, men kan vidgas till att även omfatta tiden mellan olika processteg.

Forensik
Forensik ger underrättelseinformation om vem, hur och varför något skedde och kan hjälpa till att förebygga kommande händelser (motsv. gripande av gärningsman).

Den IT-forensiska kärnan
De tre grundpelare som en IT-forensisk utredning vilar på är aktivitet, resultvärde och tid:

Aktivitet - Det gäller all aktivitet som förekommer i ett datorsystem, både processer och eventuella angripares, men även den egna aktiviteten vid den forensiska undersökningen. Aktiviteten påverkar systemet och dess data och försätter det i nya tillstånd. Det är dessa tillstånd och information rörande dem som är viktiga att ta tillvara.

Resultatvärde – I och med att det inom den IT-forensiska sfären ofta saknas tydliga och enskilt helt avgörande bevis för den eventuella otillåtna aktivitet som förekommit i ett system är det viktigt att ha värdet på resultaten (bevisen) i åtanke när de samlas in. De måste vara otvetydiga och klara. Därför bör till exempel de loggningsmekanismer som används i ett system i förväg analyseras ur ett forensiskt perspektiv, så att loggposternas värde är känt. Det underlättar väsentligt
i ett skarpt läge när snabba beslut måste fattas om vad som behöver sparas eller inte.

Vikten av snabb avbildning av data vid omhändertagande har ökat i och med att flashbaserad lagringsteknik, såsom SSD, USB-minnen m.m., blivit allt populärare. Mekaniska hårddiskar som inte är strömsatta behåller data under lång tid. Flashbaserad lagringsteknik däremot tappar i ogynnsamma fall data redan efter några veckor. Enligt JEDEC:s krav måste tillverkare av SSD för professionellt bruk (eng. enterprise) garantera att data inte blir korrupt inom i medeltal tre veckor om disken inte är strömsatt och förvaras i samma temperatur som vid drift. En avbildning av disken måste alltså göras inom det tidsspannet. Förvaras disken varmare än vid drift försvinner data ännu fortare. En utdragen tid från omhändertagande till avbildning ger också möjlighet för angripare att radera data på distans, där så är möjligt.

Vad kan göras?

De åtgärder som systemägare med flera kan göra är framför allt att i förväg planera de åtgärder som ska vidtas vid en framtida IT-forensisk utredning i det egna systemet. Planen bör göras med utgångspunkt i den IT-forensiska kärnan och belysa ansvar och åtgärder vid ett dataintrång, relevant utrustning, hur och vilka data i den som ska avbildas och vilka verktyg som ska användas för detta. Det är också viktigt att så noggrant som möjligt logga de åtgärder som vidtas, så att det går att avgöra i efterhand om, när och hur data eventuellt har påverkats.
Tillståndet och innehållet bör bevaras för så stor del av systemet som möjligt utan att kostnaden för eventuella driftavbrott därför blir för stor. Vid avbildning av lagringsmedia bör:
☐ Originalet skrivskyddas
☐ Kända och funktionsvaliderade verktyg användas
☐ Hash summor beräknas före och efter avbildning för att säkerställa att originalet är opåverkat och att avbilningen är korrekt
☐ Händelser och vidtagna åtgärder loggas så noggrant som möjligt
☐ Även icke-beständig lagring som RAM etcetera avbildas.

Vilken utrustning omfattas?

Den utrustning som omfattas varierar från system till system och därför måste varje system betraktas som unikt. Det går alltså inte att ge mer än generella råd om vilken utrustning som bör avbildas vid en IT-forensisk utredning. Generellt sett kan all utrustning som innehåller något slags minneskrets vara aktuell. Det gäller naturligtvis lagringsmedia såsom hårddiskar och USB-minnen, men även till exempel switchar, routrar, mobiltelefoner och skrivare. Inom den cyberfysiska världen är det standarddatorutrustning i det administrativa systemet som än så länge är den mest värdefulla, men det finns redan processnära utrustning, till exempel PLC:er, som liknar datorer till uppbyggnad och funktion och som mycket väl kan innehålla data som är värd att ta till vara.

Tid – De aktiviteter som förekommer i ett system måste gå att åtskilja på något sätt och kunna sättas i relation till varandra ur ett tidsmässigt perspektiv. Därför är det viktigt att all aktivitet tidsstämplas. Det är inte alltid nödvändigt att tidsstämpeln visar kalendertid, i vissa fall räcker det med att ordningsföljden på aktiviteterna kan säkerställas. Kalendertid är dock om möjligt att föredra. I och med att internet spänner över alla tidszoner i världen är det även bra om den tidszon som kalendertiden gäller finns med i tidsstämpeln. Grundpelarna ska genomsyra allt IT-forensiskt arbete och även den analys och planering som bör göras i förväg.

Kontakta Myndigheten för samhällsskydd och beredskap

651 81 Karlstad

Kontaktpersoner:
Fax: 010-240 56 00
registrator@msb.se
www.msb.se

Sabrine Wennberg
ics@msb.se

Gustav Söderlind
ics@msb.se