



---

## Security Audit.

---

### **Inleiding:**

Een audit is meestal een gebeurtenis die huivering wekt bij de betrokkenen want het betekent dat een externe organisatie een officieel onderzoek uitvoert op één of meerdere onderdelen van de firma. In tegenstelling tot de gekende financiële audits die zich richten op de financiële gegevens en hoe deze gebruikt worden, richt een Security Audit in de informatica er zich op hoe de confidentialiteit, beschikbaarheid en integriteit van de elektronische informatie van een firma verzekerd kan worden. Wat zou moeten. Een Security Audit is de beste manier om beveiliging van informatie te bepalen zonder de prijs te moeten betalen van een inbreuk hierop.

### **Waarom beveiligen ?**

Informatie is een bezit van een organisatie, een bezit met een bepaalde waarde, een waarde die u liever niet wil verliezen. Het is dan ook niet meer dan normaal dat u dit, net als andere belangrijke bezittingen van de organisatie, wenst veilig te stellen met gepaste maatregelen om het voortbestaan niet in gevaar in te brengen.

### **Inhoud van een Security Audit:**

Nogal dikwijls wordt "penetratie test" gelijk gesteld met een Security Audit. Dit is echter niet het zelfde. Een penetratie test is slechts een onderdeel zijn van een Security Audit die zich toespitst op het zoeken van eventuele beveiligingshiaten in, typisch internet, communicatie systemen die het bedrijf verbinden met de buitenwereld (Firewall, web servers, ....).

Een Security Audit gaat verder. Het is een systematisch onderzoek van systemen en procedures en hoe deze gebruikt worden. Daarom is het nodig dat de auditor kennis heeft van de organisatie en hoe ze werkt.

Security Audits gebeuren niet zomaar, ze maken deel uit van het doorlopende proces in het bepalen en onderhouden van beveiligingsmaatregelen. Dit gebeurt niet in een vergaderzaal. Het betreft iedereen die op een elektronische manier toegang heeft tot de informatie van het bedrijf. Gezien de dynamische natuur van informatica systemen, hun configuratie en het gebruik ervan kan men zich afvragen of men wel ooit alle beveiligingsaspecten kan nagaan. Security Audits is zo een middel. Een bruikbare en meetbare manier om te onderzoeken hoe veilig een omgeving werkelijk is.

Het onderzoek wordt uitgevoerd door middel van interviews, testen, onderzoek van operating systeem instellingen, analyse van netwerk shares en het nagaan van historische gegevens. De voornaamste bezorgdheid is hoe de beveiligingsmaatregelen – de bouwstenen van een degelijk beveiligingsbeleid – uitgevoerd worden.



Op een aantal vragen zal tijdens de audit geprobeerd worden een antwoord te krijgen :

- Zijn paswoorden eenvoudig te breken ?
- Hoe zit het met de beveiliging van de toestellen die toegang geven tot informatie ?
- Worden er gegevens geregistreerd van wie toegang neemt tot bepaalde informatie ?
- Worden deze gegevens opgevolgd ?
- Is de beveiliging van een systeem ingesteld volgens de regels van de kunst ?
- Zijn er onnodige toepassingen of services aanwezig ?
- Zijn operating systemen en de gebruikte toepassingen up-to-date ?
- Hoe wordt er omgegaan met backup media ?
- Wat met een contingency plan ?
- Hoe zit het met encryptie van informatie ?
- Zijn alle toepassingen in overeenstemming met het beveiligingsbeleid ?
- Hoe zit het met documentatie ?

Dit zijn slechts enkele van de vragen die kunnen en moeten gesteld worden. Enkel eerlijke en juiste antwoorden kunnen een inzicht geven in de werkelijke beveiliging van informatie.

### **Beveiligingsmaatregelen:**

Zoals reeds aangehaald is een Security Audit een middel om na te gaan hoe effectief beveiligingsmaatregelen zijn toegepast. Dit veronderstelt natuurlijk dat er beveiligingsmaatregelen genomen zijn, wat jammer genoeg nog steeds niet altijd het geval is.

Beveiligingsmaatregelen zijn een middel om de beveiliging te beschrijven zodat iedereen van het bedrijf er notie van kan (moet) nemen, begrijpen en toepassen. Indien niet iedereen op de hoogte is van de maatregelen zal het uiteraard zeer moeilijk zijn, zonet onmogelijk, om deze maatregelen toe te passen.

Er is een natuurlijke spanning tussen de cultuur op een werkplaats en beveiligingsmaatregelen. Zelfs met de beste bedoelingen kiezen werknemers vaak gemak boven veiligheid. Beveiligingsmaatregelen zijn dan ook een levende materie die steeds ter discussie kunnen en moeten staan en in een evenwicht moeten zijn met werkbaarheid.

### **Pre-audit:**

Voor men zelfs maar een audit kan uitvoeren moet men zijn huiswerk maken. Men moet weten wat men audit. Samen met het nakijken van de resultaten van een eventueel vorig onderzoek gaat men bepaalde hulpmiddelen willen gebruiken of er naar verwijzen. De eerste stap is een onderzoek ter plaatse. Dit geeft een technische beschrijving van de omgeving. Het bevat ook het in kaart brengen van het beheer en de gebruikers. Vragenlijsten kunnen een volgende stap zijn. Deze vragenlijsten geven van nature uit subjectieve informatie, maar geven wel een goed beeld van hoe de beveiligingsmaatregelen ervaren worden. De in vraag gestelde maatregelen hebben meestal betrekking op: beheersmiddelen en procedures, authenticatie/toegangscontrole systemen, fysieke beveiliging, toegangsmogelijkheden van buiten uit, verbindingen naar externe systemen, reactie op inbreuken en contingency planning.



De bedoeling is te komen tot een waarde toekenning van vastgestelde parameters met een vooropgesteld gewicht en de eventuele kost.

Best dat men ook onderzoek doet naar inbreuken uit het verleden om zo een idee te krijgen van de gekende zwakheden in het beveiligingsbeleid van de organisatie. Daarbij aansluitend onderzoekt men de huidige situatie om herhaling te voorkomen.

Gezien de hoeveelheid aan gegevens die kan (moet) verwerkt worden wordt best op voorhand de doelstellingen van en de onderworpen systemen aan de audit, in samenspraak met de klant, duidelijk afgebakend. Factoren die hierin een bepalende rol spelen zijn: het business plan van de organisatie, het type van informatie die beveiligd wordt en welk zijn waarde/belangrijkheid is in de organisatie, vorige inbreuken, de mogelijke impact van inbreuken en de beschikbare tijd om de audit uit te voeren.

Hierop aansluiten wordt er een audit plan opgesteld. Dit plan zal voorzien hoe de audit dient uitgevoerd te worden, wie betrokken gaat worden, met welke hulp middelen en wanneer. Er dient rekening gehouden te worden op welke wijze dit de dagelijkse werking kan/mag beïnvloeden.

#### **De audit:**

Wanneer de audit begint is het niet de bedoeling om het dagelijkse werk stop te zetten. Er zal duidelijk gecommuniceerd worden wat de doelstellingen zijn en hoe dit gaat uitgevoerd worden rekening houdend met eventuele stress van het moment maar met het in achtneming van het ontwerp.

De auditor moet degelijk en eerlijk te werk gaan, hierbij consistent de standaarden en procedures toepassend. Tijdens de audit zullen er gegevens vergaard worden van de fysische beveiliging van computer materiaal en zullen er interviews afgenomen worden van het betrokken personeel. Men gaat de netwerk configuratie, operating systemen en toepassingen, toegangs/authenticatie mechanismen, ... evalueren.

Gedurende dit proces wordt een check list afgewerkt maar blijft men ook alert voor toestanden die afwijken van de verwachtingen.

#### **Post-audit:**

Eventueel hoog dringende probleem situaties worden onmiddellijk gemeld zodat er onmiddellijk kan ingegrepen worden.

Nadien wordt de verzamelde informatie geanalyseerd en aan een verder onderzoek onderworpen. Hieruit zal een rapport vloeien dat zowel de positieve als negatieve bevindingen weergeeft, de mogelijke gevolgen en een voorstel tot verbetering.

De auditor kan bijstaan in het tot stand komen van de oplossing en/of mogelijke verbeteringen.



**Opvolging:**

Organisaties wijzigen en dat is ook zo voor hun beveiligingsbehoefte. Beveiliging is géén eenmalige taak maar een continu proces om informatie beter te beveiligen. Een audit geeft het huidige beveiligingsbeleid en de toepassing ervan weer. Uit de historiek van audits kan men de zwakke punten van het beleid terugvinden en bijsturen.

Tools zijn belangrijk in het uitvoeren van een audit, het is echter minder belangrijk om de laatste en meeste geweldige tool te gebruiken dan wel de juiste informatie te verzamelen, te interpreteren en de juiste conclusies te maken.

**Security Audit in 8 stappen** ( + % van totaal benodigde tijd voor uitvoering)

1. Voorbereiding	10%
2. Nakijken beleid en documenten	10%
3. Gesprekken/interviews	10%
4. Technisch onderzoek	15%
5. Onderzoeken verzamelde gegevens	20%
6. Rapportering	20%
7. Voorstelling rapport	05%
8. Post-audit acties	10%