Veiligheidstips voor beheerders van websites

Dit is maar een greep uit de bestaande technieken om risico's te beperken, natuurlijk zijn er nog duizenden anderen en hebben we ons beperkt tot de meest courante.

Hou er gewoon altijd rekening mee dat het internet ook gevaren inhoudt en dat je bewust moet omspringen met wat je in je professionele leven dagdagelijks doet. Dat betekent dat je deze informatie ook binnen openbare en professionele kringen voor jezelf moet houden, daar het web de grootste vergaarbak van informatie is en de hacking community deze info vergaart, correleert en misbruikt.

1. Lees even 'De tien geboden voor veilig surfen op het World Wide Web'

2. Aanleveren van inhoud

Een van de mogelijke tegenmaatregelen om te voorkomen dat foutieve content op het web gepubliceerd wordt, is het inbouwen van een goedkeuringsworkflow. Dit wordt in het jargon het 'vier ogenprincipe' of 'segregation of duties' genoemd en houdt in dat een andere persoon een bijkomende validatie uitvoert voor de data op het net komt.

Welke risico's beperk je hiermee?

Hiermee beperk je het risico dat er verkeerde info op het net komt met mogelijks financiële of reputatieschade tot gevolg.

3. Identificatie- en authenticatiemiddelen

Identificatie is de manier waarbij er aan iemand een identiteit wordt toegekend. Dit is een proces dat afhankelijk is van het risico van je toepassing, waarbij de zekerheid van de link tussen de identiteit en de persoon van een hoog of laag niveau moet zijn. Het gaat om de garantie dat de persoon wel degelijk de persoon is waarvoor hij zich uitgeeft. Enkele voorbeelden:

- je kan een usernaam uitreiken aan een persoon ermee rekening houdend dat de persoon zich ergens aan de andere kant van de wereld kan bevinden. Je biedt daartoe een registratiepagina aan waarop de persoon in kwestie enkel een e-mailadres achterlaat met eventueel een CAPTCHA. Daarna stuurt de registrator een mailtje uit om het proces voor het bekomen van een identiteit af te ronden. Dit is een **heel zwak** proces
- nagenoeg hetzelfde proces, maar men werkt met een bijkomende databank van geaccrediteerde personen en intern voert iemand bijkomende controles uit eventueel via een ander kanaal bijvoorbeeld een telefonische oproep. Hiermee worden enkele basiscontroles uitgevoerd. Ook dit is nog altijd een **zwak** proces

- een burger gaat met de nodige bewijsstukken zijn elektronische identiteitskaart of zijn bankkaart afhalen op het gemeentehuis of bankkantoor. Deze persoon biedt zich fysiek aan zodat de ambtenaar of bankbediende de identiteit kan controleren. Dit is een **sterk** proces
- Nog andere processen zijn mogelijk.

Een **authenticatiemiddel** gaat over het algemeen over iets dat je bezit, bijvoorbeeld een usernaam, in combinatie met iets dat je kent zoals een wachtwoord. Er zijn meerdere combinaties mogelijk :

- gebruikersnaam en wachtwoord
- éénmalige wachtwoorden of 'One Time Passwords' (OTP). Dit kan gaan van een app op je smartphone, bijvoorbeeld een 'Google authenticator', tot een combinatie die via SMS wordt aangereikt
- de smartcards waarbij een private sleutel is ingebakken, gecombineerd met een sterk uitreikingsproces in combinatie met een pin-code. Voorbeelden hiervan zijn de eID en de bankkaart
- 'TAN-lijsten' zijn een lijst van combinaties op papier die kunnen variëren afhankelijk van de keuze van de implementator. Een voorbeeld hiervan is het token in België
- Er zijn nog andere mogelijkheden

Het authenticatiemiddel en het uitreikings- en validatieproces zijn onlosmakelijk verbonden met het veiligheidsniveau dat vereist is vooraleer toegang verleend kan worden. Je kan deze factoren dus niet los van elkaar zien.

Probeer daarom deze eenvoudige stelregel te hanteren: verdeel het paswoord, pin, tan, smartcard en de uitgereikte identiteit altijd over verschillende zendingen, smsjes of e-mails en gebruik altijd verschillende kanalen. Zorg er altijd voor dat één tussenpersoon ook bij de uitreiker alle informatie in handen heeft.

Enkele voorbeelden van hoe het mis kan gaan :

- een gebruikersnaam- en wachtwoordcombinatie van 8 karakters bestaande uit een woord uit een woordenboek, bijvoorbeeld 'huiswerk' kan eenvoudig achterhaald worden met een zogenaamde 'dictionary attack'. Hierbij wordt gebruik gemaakt van een set van woorden, of bijvoorbeeld van een woordenboek en de combinaties van de woorden. Bij een online aanval kunnen de hackers binnen de 3 uur de combinatie kraken. Wanneer ze de databank hebben, is dat al binnen enkele seconden het geval, afhankelijk van de rekenkracht wel te verstaan.
- Probeer de data van gebruikers bij gebruiker/wachtwoordcombinaties, die meestal centraal opgeslagen zijn, altijd te encrypteren met versleuteling van een voldoende hoog niveau. Indien de databank gehackt wordt, heb je een groot risico dat je snel veel imagoschade hebt en dat je data niet meer integer of confidentieel is. Dit heeft als bijkomend gevolg dat je de dienst moet stoppen voor onbeperkte tijd.

Welke risico's beperk je hiermee?

Indien je rekening houdt met wat hierboven beschreven is en je de stappen weloverwogen implementeert, beperk je het risico op het vlak van beschikbaarheid, reputatie, financiële gevolgen en confidentialiteit.

4. Controle houden op de users

Controle houden op rechten van gebruikers is cruciaal, omdat een gebruikersgemeenschap een levend gegeven is. Mensen en organisaties zijn onderhevig aan wijzigingen: mensen komen en gaan, veranderen van functie, gaan met pensioen en ga zo maar door. Dit aspect heet in het jargon User Life Cycle.

Om deze levenscyclus onder controle te houden is het cruciaal om enkele controles in te bouwen zoals :

- probeer voor het aanmaken van een gebruiker een workflow te gebruiken die een andere persoon moet valideren vooraleer een recht wordt toegekend aan een persoon
- Mensen die administratieve taken op zich nemen zoals het aanmaken van gebruiker/wachtwoorden kunnen beter een ander en hoger authenticatiemiddel gebruiken, bijvoorbeeld de eID
- Geef nooit wachtwoorden en gebruikersnamen door aan elkaar, zeker niet in de elementen waar het vier ogen principe wordt toegepast
- Gebruik waar mogelijk stringente wachtwoordregels
- Auditeer de uitgereikte rechten op periodieke basis. De controle wordt het best uitgevoerd door een andere persoon dan diegene die de rechten heeft toegekend

Welke risico's beperk je hiermee?

Je beperkt hierdoor het risico dat toegekende rechten blijven bestaan nadat een gebruiker de organisatie heeft verlaten en dat de user life cycle niet meer integer is.

5. Zwakheden op systemen en toepassingen

Voer als organisatie regelmatig veiligheidsscans uit op de systemen zoals computers, laptops, servers en toepassingen, met een zwakhedenscan. Volg voor de specifieke omgevingen die ter beschikking staan van de organisatie de zwakheden op die te vinden zijn op exploit-db.com en www.security focus.com, cert.europa.eu, www.us-cert.gov en andere website.

Maak bovendien gebruik van de standaard firewall en ook van firewalls op het niveau van de toepassingen. Maak gebruik van technieken en inbraakdetectiesystemen om gekende aanvallen te beperken en volg op regelmatige basis de loginformatie op, daar deze info heel nuttig kan zijn om profielen te detecteren.

Welke risico's beperk je hiermee?

Hiermee beperkt je de impact van dataverlies, malware, spionage, beschikbaarheid en andere problemen.

6. Gebruik sterke wachtwoorden, hergebruik ze niet, deel ze nooit en vernieuw ze regelmatig

De gouden regel is: hoe langer en complexer het wachtwoord, hoe veiliger.

Gebruik een wachtzin in plaats van een woord: een lange zin is eenvoudig om te onthouden én veiliger.

Je kan ook een beroep doen op programma's, de zogenaamde 'wachtwoordkluizen', om het wachtwoord voor jou aan te maken en te onthouden.

Hernieuw op regelmatige basis je wachtwoorden. Probeer bij registratie op websites steeds andere wachtwoorden en mailadressen te gebruiken.

Naast je wachtwoord geef je bijvoorbeeld ook een code in die alleen jij via je gsm toegestuurd krijgt. Deze mogelijkheid kan je vaak zelf activeren binnen het programma of bij de website waarmee je werkt.

De antwoorden op geheime vragen die je kan invullen om je wachtwoord extra te beveiligen of te resetten, zijn eenvoudig te raden. Moet je dit toch invullen, dan antwoord je best niet op de vraag, maar geef je een fictief antwoord. Onthoud dit zelf goed of maak gebruik van een wachtwoordkluis.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact in het geval er misbruik van je account en maak je het hackers moelijker om op het net gehackte wachtwoorden en accounts te hergebruiken.

7. Het gebruik van SSL

Wanneer https:// in je browser staat als begin van je internetadres, dan werk je met een beveiligde verbinding. Indien je een foutmelding krijgt dat het certificaat niet correct is, dan is deze verbinding niet meer veilig.

Houd ook steeds je SSL-implementatie up-to-date. Sinds 2013-14 is SSL enkele zwakheden beginnen vertonen. Hierdoor konden wereldwijd miljoenen websites afgeluisterd worden. Het betekent dus niet dat met de implementatie van SSL de klus voor eeuwig en altijd geklaard is. Dit geldt evenzeer voor de sterkte van de versleuteling die je gekozen hebt op een bepaald ogenblik in de tijd.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact van dataverlies en afluisteren van de verbinding.

8. Beveilig steeds je Wi-Fi-netwerken

Beveilig je netwerk thuis of op kantoor met een wachtwoord en laat dit regelmatige wijzigen. Wees voorzichtig met publieke Wi-Finetwerken. Wantrouw deze altijd en probeer je taken in alle omstandigheden altijd over een beveiligde verbinding uit te voeren via VPN-technologie.

Zo kan niemand, of het nu cybercriminelen of je buren zijn zoals bijvoorbeeld andere bedrijven in hetzelfde kantoor of andere personeelsleden, gebruik maken van je draadloos internet.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact van dataverlies en het afluisteren van de verbinding.

9. Zorg dat het geheugen van je toestel en of server volledig gewist is

Het geheugen van je smartphone of tablet maak je leeg via de optie "wissen" op je toestel. Je computer of laptop wis en formatteer je best volledig. Je kan dit snel of uitgebreid laten uitvoeren door de ICT-departementen. Een snelle “format” is geen goed idee, dan blijven er altijd gegevens achter.

Welke risico’s beperk je hiermee?

Hiermee beperk je de impact van dataverlies en voorkom je dat gebruikersnamen en wachtwoorden in de verkeerde handen vallen.

10. Back-up en restoreprocedure

Zorg dat je systemen en gegevens altijd een back-up hebben. Controleer altijd de correctheid van je back-up en voer op regelmatige tijdstippen, bijvoorbeeld voor een site live gaat, een restoreprocedure uit. Voer minimaal 2 maal per jaar een restoreprocedure uit van de back-up en valideer de juistheid van de restoreprocedure.

Beveilig ook je back-ups daar deze dezelfde info bevatten als je data die zich op de verschillende omgevingen bevindt.

Documenteer in de mate van het mogelijk zeker de wijze waarop een back-up- en restoreprocedure verloopt opdat ook mensen die geen kennis hebben van de omgevingen de restoreprocedure succesvol kunnen uitvoeren.

Welke risico’s beperk je hiermee?

Hiermee beperk je de impact van dataverlies en beschikbaarheid.

Bronnen

(https://www.safeonweb.be/nl/tips)

(https://cert.europa.eu/cert/alertedition/en/malware.html)

(https://pentestmag.com/the-cyberwar)