

# Applicatiebeveiliging

## Een Chinese Muur rond uw applicatie of database

**Inbrekers die een bedrijfspand of woning op het oog hebben, zoeken naar de zwakste schakel om binnen te komen. Bij netwerken en applicaties is dit niet anders. Maar in de meeste gevallen zit de voordeur bij IT-omgevingen nu wel op slot dankzij antivirussoftware en firewall-oplossingen. Dus richten hackers zich nu op de achterdeuren. Die staan nog te vaak open. Daarom biedt Motiv nu een pakket aan diensten en oplossingen waarmee bedrijven ook hun applicaties optimaal kunnen beschermen tegen bedreigingen.**

Dat is nodig nu kwaadwillenden proberen bestaande beveiligingssystemen te omzeilen. Zij maken daarbij gebruik van zwakke punten in de applicaties. Hierbij moet worden gedacht aan componenten zoals gebruikersinterface, onderliggende API's of het file systeem die vaak nog onbeschermd zijn. Maar juist deze componenten maken het mogelijk om een applicatie te benaderen en dus te manipuleren. Bij een ongeoorloofde wijziging zal bijvoorbeeld een standaard firewall geen onregelmatigheid opmerken.

Het belang van een nieuw type firewall voor applicatiebeveiliging ligt voor de hand. Databases en de applicaties bevatten voor de meeste bedrijven en organisaties de meest bedrijfskritische informatie. Wanneer deze niet beschikbaar zijn, of niet goed functioneren, loopt de schade snel op. Daarnaast bieden ze voor cybercriminelen interessante manieren om met persoonlijke gegevens te frauderen of identiteiten van anderen aan te nemen. Ook dan is de schade – zeker voor bedrijven – aanzienlijk.

In deze gevallen biedt een standaard firewall niet altijd de optimale bescherming die nodig is, bijvoorbeeld bij websites voor telebankieren of bestelsites die toegang bieden tot elektronisch winkelen. Applicatie-firewalls zorgen hier voor extra bescherming en bieden daarnaast nog een ander cruciaal voordeel. Doordat ze alle acties vastleggen en deze voorzien van een tijdstempel, is altijd te achterhalen welke acties op welk moment plaatsgevonden hebben en wie ze heeft uitgevoerd. Daarmee kan een organisatie voldoen aan bepaalde compliance-regels en kunnen de verzamelde gegevens als officieel bewijs dienen wanneer regels zijn overtreden.

### Waarom applicatiebeveiliging?

De meeste applicaties zijn beschermd met een firewall. Ook alle security patches van het operating systeem en de web services worden meestal tijdig geïnstalleerd. Daarom maken hackers steeds vaker gebruik van specifieke zwakheden in de applicatie. Hieronder enige voorbeelden van mogelijke kwetsbaarheden op applicatieniveau:

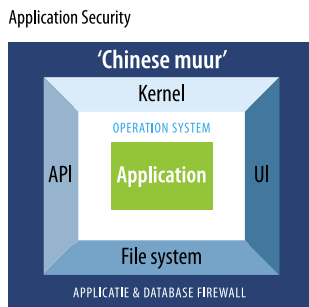
- Cross-site scripting (XSS) is een benaming voor een type bedreiging voor de beveiliging van computers die in webapplicaties kunnen voorkomen. Hetzelfde bron principe zegt dat een script van de ene bron niet de pagina en gegevens, zoals cookies, van een andere bron mag lezen of wijzigen. Wanneer een aanvaller hetzelfde bron principe voor HTML-scripting probeert te omzeilen spreekt men van cross-site scripting.
- Een bufferoverflow (Engels: buffer overflow) is een foutief gedrag van een computerprogramma dat probeert data te schrijven in een tijdelijke gegevensruimte maar buiten de grenzen van deze buffer schrijft. Dit veroorzaakt in de meeste gevallen een stopzetting van het programma. Fouten in zulke programma's, maar nog meer in het geval van besturingssystemen, worden soms misbruikt door wormen, virussen en hackers om ongeoorloofde toegang te krijgen tot computersystemen.
- Een man-in-the-middle-aanval is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. De berichten kunnen daarbij mogelijk gelezen en/of veranderd worden. Ook kunnen berichten worden verzonden die niet door de andere partij zijn geschreven. De naam van de aanval verwijst naar de derde persoon die in het midden tussen de twee partijen 'staat' en de langskomende berichten bekijkt en/of aanpast.
- SQL injectie is een aanval waarbij applicaties SQL-queries genereren aan de hand van input van gebruikers. Vanuit de gebruikersinterface van een web-applicatie kan door middel van gemanipuleerde SQL commando's een ongewenste applicatie of query worden geladen/gestart in een database.



## Applicatiebeveiliging - een Chinese muur rond uw applicatie of database

### Chinese Muur zorgt voor applicatiebeveiliging

Een informatiesysteem bestaat uit diverse componenten waaronder applicatiesoftware, een besturingssysteem en hardware. Voor beveiliging van een compleet informatiesysteem wordt de applicatiesoftware als de kern gezien. Daaromheen ligt de schil van het besturingssysteem en de hardware. Naast de gebruikersinterface van de applicatie wordt vanuit beveiligingsoogpunt gekeken naar alle in- en uitvoer op deze componenten. Dus ook alle acties op het gebied van I/O, API's en het bestandssysteem. Een Chinese Muur rondom het complete informatiesysteem zorgt voor complete applicatiebeveiliging. Aan de hand van een black list of white list worden acties wel of niet toegestaan. Doordat alle acties gecheckt worden, is er in feite een Chinese Muur om de applicatie plus database heen gelegd. Naast controles zorgt een applicatie en database firewall ook voor uitgebreide logging en monitoring.



### Aanpak

Motiv start de projecten op het gebied van applicatiebeveiliging met een intake. Daarin stellen we nauwkeurig de eisen en wensen van de organisatie vast. Naast de vraag naar applicatiebeveiliging wordt bijvoorbeeld ook gekeken in hoeverre logging conform policy compliancy moet worden bewaard. Vervolgens zorgen we voor de set-up en installatie van de appliances. In nauw overleg met de klant stellen we de policies vast en implementeren we deze. De appliance kan vervolgens getest worden, waarna fine-tuning plaatsvindt. De analyse van de logging kan aanleiding zijn voor het verscherpen van de regels. Het optimaliseren van de application level firewall is een continu proces. Om die reden adviseert Motiv periodiek op locatie van de klant. Deze adviezen worden uitgevoerd met applicatie- of database-specialisten van Motiv. Met onze totale security kennis op netwerken, databases en web services beschikken we over alle expertise voor applicatie- en database-beveiliging.

### Partners Imperva en Cenzic

Imperva is marktleider op het gebied van netwerkbeveiliging voor web-services en databases. Doordat continu nieuwe kwetsbaarheden in bestaande databases, applicaties, cryptografie en web bekend worden, is het vrijwel onmogelijk om de beveiliging van gevoelige of interne informatie in databases te kunnen waarborgen. Met de toenemende wet- en regelgeving zoals Basel II wordt beveiliging tegelijkertijd steeds belangrijker.

SecureSphere productlijn van Imperva voorziet in een totaaloplossing voor extra bescherming tegen interne bedreigingen, externe bedreigingen zoals web attacks, kwetsbaarheden in databases en bescherming tegen Internet-wormen. Imperva wordt ingezet voor als maximale beveiliging zoals bij e-commerce en Internet-bankieren noodzakelijk wordt geacht.

Voor het testen van beveiliging tijdens het ontwikkelproces werkt Motiv samen met Cenzic, dat met zijn product Hailstorm een oplossing biedt voor het testen van web-applicaties op eventuele beveiligingslekken.

### Motiv: Professioneel en eigenzinnig

**U heeft een netwerk- of databaseprobleem en zoekt een sparringpartner? Of u wilt nieuwe webtechnologie of een beveiligingsoplossing integreren in uw bestaande infrastructuur? Misschien heeft u gewoon een complex technisch probleem met uw IT-infrastructuur, dat opgelost moet worden.**

**In al deze gevallen is Motiv u graag van dienst. Want ons uitgangspunt is, dat elke klant anders is. En daarom zijn we voor de ene klant een sparringpartner en voor de andere een systems integrator. Bij weer een andere klant zorgen we er gewoon voor dat een probleem snel wordt opgelost. In welke rol u ons ook inschakelt, wij kijken altijd naar de veiligheid van uw infrastructuur en systemen. Want data- en systeembeveiliging loopt als een rode draad door onze activiteiten.**

### Motiv

Poortdijk 13

NL - 3402 BM IJsselstein

[www.motiv.nl](http://www.motiv.nl)

[info@motiv.nl](mailto:info@motiv.nl)

T +31 [0]30 - 68 77 007

F +31 [0]30 - 68 77 006