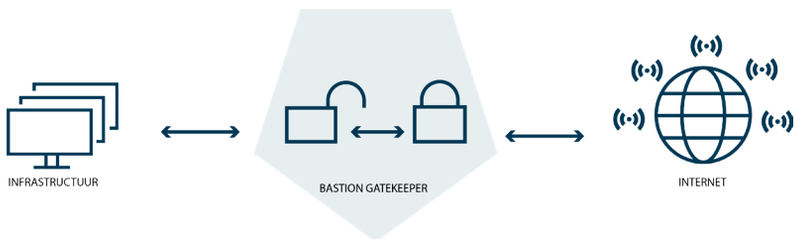
BASTION GATEKEEPER

Bastion Gatekeeper

In een ideale wereld (en conform menig vigerend beveiligingsbeleid) is een infrastructuur niet of onder zeer strenge voorwaarden (beperkt) gekoppeld met het internet. Dat conflicteert steeds vaker met de alsmaar toenemende behoefte om informatie overal vandaan te kunnen ontvangen, te verrijken en/of te delen met gebruikers die zich niet op een locatie bevinden waar ze fysiek toegang hebben tot de infrastructuur of waar de vereiste beveiligingsmaatregelen (ongeacht of dit nu om organisatorische, bouwkundige of elektronische maatregelen gaat) niet kunnen worden gerealiseerd. Steeds meer organisaties worstelen met dit gegeven en zoeken naar manieren om toch veilig informatie te kunnen ontsluiten terwijl er een onmiskenbare toename is in de digitale dreiging.

In de Bastion filosofie is het uitgangspunt niet óf maar wannéér een organisatie wordt aangevallen. Door van dit uitgaanspunt uit te gaan bij het ontwerpen en implementeren van alle relevante beveiligingsmaatregelen ontstaat een hele nieuwe benadering. In deze benadering is niet één maatregel voldoende maar zit de kracht in de combinatie van meerdere elkaar versterkende beveiligingsmaatregelen die samen de beschikbaarheid, integriteit en vertrouwelijkheid van de vertrouwelijke informatie garanderen.



Om uw bedrijfsnetwerk veilig te koppelen aan het internet is Bastion Gatekeeper ontwikkeld. Hiermee krijgt u een gestandaardiseerde oplossing voorzien van een, op basis van kennis, kunde en ervaring, ontworpen koppelvlak, voorzien van een krachtige set van maatregelen, die aan de rand van uw netwerk een veilige koppeling met het internet verzorgt. Om dit te realiseren maakt Bastion Gatekeeper gebruik van defense in depth, zero trust, segmentatie en uitgebreide detectiemogelijkheden.

TEDAS
SENSE FOR SAFETY

BASTION GATEKEEPER

Defense in depth

De gebalanceerde set van maatregelen voorziet onder andere in defence in depth, uitgebreide (on)zichtbare detectiemogelijkheden en logcorrelatie over netwerksegmenten heen waardoor er een reële kans is op detectie ruim voordat het beoogde doel van de inbraak wordt bereikt en beschikbaarheid, integriteit en vertrouwelijkheid van de vertrouwelijke informatie geborgd blijven. Voor systemen die publiek beschikbaar moeten zijn kan met behulp van Cloud Computing aanvullende diepte worden gerealiseerd om ook de weerbaarheid tegen Distributed Denial of Service (DDoS) aanvallen te verhogen en de beschikbaarheid van de (achterliggende) infrastructuur te garanderen.

Zero trust

In Bastion Gatekeeper gaan we uit van zero trust. Er is geen onderscheid is tussen de interne en externe (doorgaans internet) zijde van een infrastructuur. Dit houdt in dat alleen vertrouwd verkeer wordt toegestaan tussen servers/services onderling en tussen servers/services en endpoints. Daarnaast is het essentieel dat, voor zover dit technisch mogelijk en haalbaar is, elke toegestane verbinding is versleuteld. Het draagt bij aan de instandhouding van de integriteit en vertrouwelijkheid van de informatie.

Segmentatie

De segmentatie in Bastion Gatekeeper zorgt dat de beschikbaarheid en vertrouwelijkheid van gevoelige informatie kan worden gegarandeerd. Bij correct uitgevoerde segmentatie is de kans op een uitbraak naar een ander segment minimaal.

Detectiemogelijkheden & Monitoring

Als zowel segmentatie, zero trust als defence in depth wordt toegepast ontstaat de ideale uitgangssituatie voor het aanbrengen van inspectie en detectiemogelijkheden. Zero trust zorgt ervoor dat alleen vertrouwd verkeer wordt verstuurd. Segmentatie introduceert knooppunten waar als gevolg van zero trust alleen vertrouwd verkeer doorheen loopt. Verkeer dat ontstaat als gevolg van een inbraak is snel te herkennen dankzij correlatie van monitoring in de segmenten en logbestanden op endpoints. Defence in depth zorgt, als gevolg van meerdere opeenvolgende plekken waar detectie plaatsvindt, voor vroegtijdige alarmering, zodat manueel of geautomatiseerd onveilige verkeerstromen kunnen worden geblokkeerd en/of servers/services kunnen worden geïsoleerd.

TEDAS
SENSE FOR SAFETY

info@tedas.nl | **www.tedas.nl**