advenica

Spårbarhet och loggning i säkerhets-känslig verksamhet

Centraliserad logginsamling i säkerhetskänsliga system medför ökad risk för attacker. För att minska riskerna krävs en lösning som skyddar både logginformation och alla anslutna system.

Utmaning

Skapa centraliserad logginsamling på ett säkert sätt

De flesta IT-system skapar loggar som möjliggör felsökning och spårbarhet. För att dra bästa nytta av sådana loggar är det viktigt att samla ihop loggar från så många system som möjligt till en gemensam kronologisk lista. Har man säkerhetskänsliga eller zonindelade system och vill genomföra centraliserad logginsamling måste man ta hänsyn till en inbyggd målkonflikt. Loggningen vinner på att ha ett gemensamt system för samtliga zoner/delsystem samtidigt som ett gemensamt system ökar risken för attacker av olika slag.

1. Risk att loggsystemet kontamineras med hemlig information

Om någon av zonerna innehåller hemlig information finns risk att även loggsystemet kontamineras med hemlig information. Om det sker ökar det totala skyddsbehovet i och med att zonen som uppgifterna kommer ifrån, såväl som loggsystemet måste skyddas mot läckage av de hemliga uppgifterna.

2. Risk att loggsystemet används som språngbräda för attacker

Om loggservern är ansluten till flera zoner blir den i sig ett attraktivt delmål för att via loggservern attackera system i en annan zon.

3. Risk att loggsystemet används för rekognoscering inför framtida attacker

I loggsystemet går det att dra slutsatser om vilka händelser som är synliga. En attackerare kan anpassa sitt sätt att genomföra en attack och därmed minska risken att upptäckas.

4. Risk att loggsystemet attackeras för att sopa igen spåren efter en attack

Om en attackerare kan komma åt loggsystemet kan denne förvanska eller radera logguppgifter, vilket påverkar logginformationens pålitlighet. Det finns också en risk att logginformationen raderas eller förvanskas redan innan den når loggsystemet.

Lösning

Enkelriktat dataflöde

Centraliserad logginsamling är en uppgift som kan skyddas på mycket kraftfullt sätt med hjälp av datadioder. Alla de zoner som levererar logginformation skyddas med en datadiod vardera. Dataflödet enkelriktas i riktning mot loggsystemet. Ett gemensamt loggsystem kan därmed utnyttjas oavsett hur många zoner som levererar data till loggsystemet. Om någon av zonerna innehåller hemlig information måste antingen loggsystemet skyddas på motsvarande konfidentialitetsnivå, alternativt måste logginformationen från en sådan zon filtreras så att loggsystemet inte kontamineras med hemlig information. Det kan dock leda till att värdet av logginformationen minskar eftersom fritextdata ofta måste filtreras bort, vilket leder till att logginformationen kan bli svårare att tolka.

- Dioderna gör det omöjligt att använda loggsystemet som en språngbräda (2).
- Tack vare dioderna är det lätt att avgränsa loggsystemet så att ingen obehörig kan ta del av informationen (1,3).
- Det blir mycket svårare för en attackerare att dölja spåren efter en attack (4).
- Det är även möjligt att kryptera förbindelsen till loggservern för att hindra förvanskning (4).

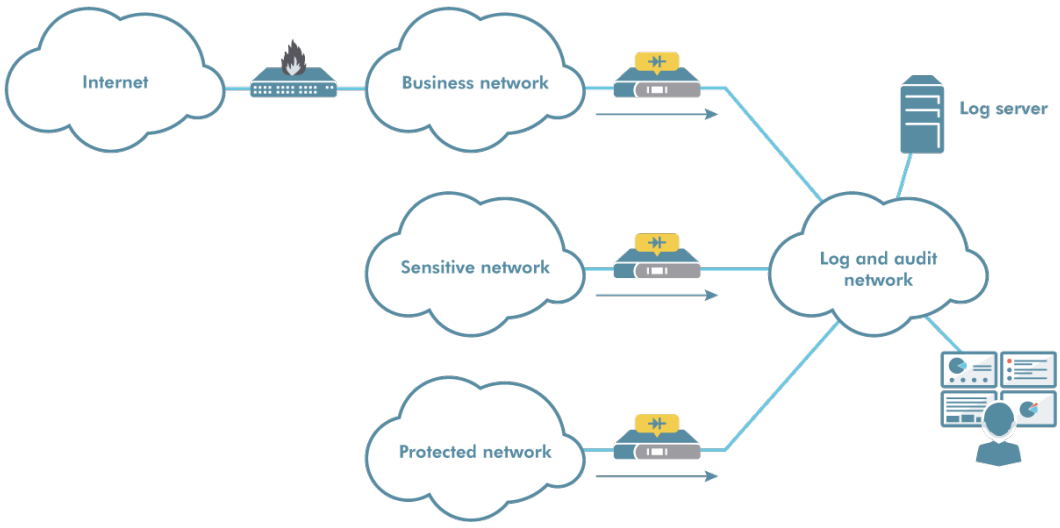
Fördelar

Skydda insamling av logginformation

Genom att använda datadioder för att skydda insamling av logginformation erhålls ett mycket gott skydd:

- Det blir omöjligt att genomföra attacker från loggsystemet in mot någon av zonerna.
- Man kan nyttja ett gemensamt loggsystem oavsett antalet zoner som är anslutna. Därmed undviks de extrakostnader som skulle blivit följden om flera loggsystem skall hållas igång parallellt.
- Man kan enkelt avgränsa och skydda loggsystemet så att ingen obehörig kan ta del av dess innehåll.
- Datadioderna medför förenklad säkerhetsanalys (och därmed förenklad driftsättning) och tillfredsställer mycket högt ställda krav från till exempel tillsynsmyndigheter.

Läs mer om våra datadioder på advenica.com.



advenica

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-inmotion upp till Top Secret-klassning. Med oss stärker länder, myndigheter och företag informationssäkerheten och digitaliserar ansvarsfullt. Bolaget grundades 1993 och har EU-godkännande på högsta säkerhetsnivå. Våra unika produkter designas, utvecklas och tillverkas i Sverige.

Läs mer på advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED