advenica

# Skydda bankers känsliga tillgångar

Cybersäkerhet för banker

# Cybersäkerhet – ert ansvar gentemot era kunder

Cyberattacker är ett ständigt hot mot myndigheter eftersom de hanterar mycket känslig information. Samma hot existerar även för banker då de hanterar många viktiga tillgångar samt känslig information.

## Digital kommunikation – snabbt, lätt och riskabelt

Digitalisering gör att fler enheter är anslutna till Internet vilket är bekvämt, men det ökar också de möjliga attackvägarna till IT-strukturen. Samtidigt blir metoderna som används av dagens angripare mer och mer förfinade och attackerna är vanligtvis riktade och välplanerade.

## Attacker med banker som måltavla

Det kan bli väldigt dyrt att inte skydda sin information. The Development Bank of Seychelles upplevde en ransomware-attack mot sitt nätverk i september 2020[1]. Under en ransomware-attack krypterar angriparen offrets filer och kräver ett lösenord för att göra dem tillgängliga igen. Detta innebär att det kan bli mycket dyrare att få tillgång till sina filer igen efter en attack än att betala för säkert skydd och därigenom undvika sådana risker.

1 CBS closely monitoring DBS' report of a ransomware attack on its network från https://www.cbs.sc/Downloads/Pressrelease/CBS%20closely%20monitoring%20DBS%E2%80%99%20report%20of%20a%20ransomware%20attack%20on%20its%20network.pdf



© Advenica 2021

Ungerska banktjänster påverkades också av en kritisk cyberattack under 2020 - en så kallad DDoS-attack (distribution-denial-of-service). Detta ansågs vara en av de största DDoS-attackerna i Ungern[2]. Under en DDoS-attack, översvämmas systemet med datatrafik av angriparna i syfte att förlama systemet. Under denna incident avbröts vissa av bankernas tjänster. Denna typ av attack kan innebära stora kostnader eftersom organisationen och eventuella kunder ofta inte kan använda hela verksamheten som blir tillfälligt förlamad.

## Nya EU-riktlinjer för banker

Eftersom så mycket står på spel kan banker inte ta risken att inte ha ett säkert skydd mot hot. Den 30 juni 2020 trädde de nya EU-riktlinjerna avseende cybersäkerhet för banker[3] i kraft. Riktlinjerna gäller finansinstitut så som betaltjänstleverantörer, kreditinstitut och värdepappersföretag.

De nya riktlinjerna från European Banking Authority, EBA, är den europeiska standarden för hantering av säkerhets- och IT-risker. Den beskriver hur banker, fondförvaltare och leverantörer av betaltjänster som är verksamma inom EU ska hantera interna och externa risker kopplade till IT och säkerhet. Dessa riktlinjer syftar till att minska sannolikheten för attacker som kan leda till dataläckage och störningar.

Riktlinjerna pekar bland annat på vilka säkerhetsåtgärder som måste utvecklas och genomföras för att minska IT- och säkerhetsrisker som finansiella institut exponeras för. Det är viktigt att förstå att riktlinjerna har rättslig grund och att de aktörer som omfattas därför är skyldiga enligt lag att kunna motivera alla avvikelser från dess tillämpning.

2 Hungarian banks, telecoms services briefly hit by cyber attack - Magyar Telekom från https://www.reuters.com/article/us-hungary-cyber/hungary-hit-by-large-cyber-attack-from-asia-magyar-telekom-idUSKBN26H0CB?il=0

3 EBA:s riktlinjer för hantering av IKT-risker och säkerhetsrisker från https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880828/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_SV.pdf

© Advenica 2021

## Vilka informationssäkerhetskrav ställer de nya riktlinjerna?

Riktlinjerna innehåller mycket information, men ett centralt krav gäller klassificering. Detta krav anger att finansinstitut måste göra en klassificering av affärsfunktioner, supportprocesser och informationstillgångar, bedömda utifrån hur kritiska dessa är.

Ett annat viktigt krav är informationssäkerhetsåtgärder; riktlinjerna anger att säkerhetsåtgärder måste utvecklas och genomföras för att minska de IT- och säkerhetsrisker som finansiella institut står inför.

*Banker kan inte ta risken att inte ha ett säkert skydd gentemot hot*

## Hur vet vi vilken information som bör skyddas?

Det är viktigt att klassificera all slags information, så att det blir tydligt hur informationen måste hanteras. För att göra klassificeringen måste du utvärdera aspekter som informationens värde och känslighet, de juridiska kraven och informationens betydelse för verksamheten. Ett bra sätt att bestämma hur klassificeringen ska göras är att använda en risk- och säkerhetsanalys. Det hjälper dig att kartlägga din nuvarande informationssäkerhet samt dina framtida behov.

## Ni behöver mer än en brandvägg

För att skydda det mest skyddsvärda och verksamhetskritiska bör en annan teknik än brandväggar övervägas. Med en brandvägg är det svårt att veta exakt vilken information som exporteras eller importeras i systemet. En brandväggs konfiguration blir ofta komplex vilket ökar risken för felkonfiguration. Brandväggar separerar inte heller administration och dataflöde på ett sätt som skyddar informationen från insiders. När brandväggar dessutom hanteras genom molntjänster innebär själva outsourcingen ytterligare riskexponering. Brandväggar fungerar ypperligt i miljöer med stora dataflöden där trafiken är

### SecuriCDS Data Diode

SecuriCDS Data Diode förhindrar inte bara intrång och upprätthåller nätverksintegritet utan förhindrar lika effektivt läckage och upprätthåller nätverkskonfidentialitet. Denna lösning med hög säkerhet skyddar tillgångar för operatörer inom bland annat kritisk infrastruktur, kommuner eller försvarsindustrin. SecuriCDS Data Diode garanterar enkelriktad åtskillnad mellan nätverksgränssnitt och kan säkert ansluta två nätverk av samma eller olika säkerhetsnivåer.

### Fördelar

- Skapar enkelriktad loggtrafik från övervakade system till loggsamlingssystemet
- Eliminerar dataläckage från loggdatasystemet, samt attackerares möjlighet att hoppa mellan system
- Aktiverar strikt segmentering medan central övervakning av system och nätverk behålls
- Gör det möjligt att använda ett enda system för datainsamling av loggar utan att äventyra säkerheten - detta minskar kostnaderna, ökar administratörens insikt och förbättrar möjligheten att upptäcka attacker och snabbt vidta motåtgärder

Advenica SecuriCDS Data Diode



© Advenica 2021

mångsidig och föränderlig, t.ex. som yttre skydd mot internet och för uppdelning i DMZ och kontorsmiljö. Det är viktigt att etablera ett djupförsvar med flera säkerhetsbarriärer mellan det mest skyddsvärda och hotaktörerna. Säkerhetsprodukter från olika leverantörer bör användas för att minska risken att samma sårbarhet finns i samtliga produkter. Konfigurationsändringar av säkerhetsprodukter bör styras upp så att ändringar föregås av granskning av fler än en person som förstår och kan godkänna ändringen.

## Nätverkssegmentering höjer säkerheten för banker

En utmärkt metod för att mildra säkerhetsrisker och skydda kritisk information och kritiska system är nätverkssegmentering genom en kombination av fysisk och logisk separation. Fysisk separation innebär att säkerhetszoner definieras och distribueras till olika fysiska hårdvaror. Logisk separation innebär att olika zoner eller nätverkstrafik får samexistera på samma hårdvara eller i samma nätverkskabel, vilket är mindre tydligt och därmed medför lägre förtroende för separationsmekanismens styrka än för fysisk separation.

*Advenicas Datadiod uppfyller både funktion och säkerhet*

Nätverkssegmentering i situationer där envägskommunikation är nödvändig, dvs. där information endast måste gå i en riktning, kan lösas med datadioder. Det viktigaste med en datadiod är att information endast kan passera i en riktning. I Advenicas SecuriCDS-datadiod baseras separationen och diodfunktionen på en optisk sändare och mottagare. Designen garanterar att ingen data överförs i motsatt riktning. Med certifierade lösningar som Advenicas SecuriCDS-datadiod, som uppfyller militära standarder, uppfylls både funktion och säkerhet.

Vi har också lösningar för nätverkssegmentering för situationer där ett tvåvägs-informationsflöde är nödvändigt. Här filtreras data effektivt och i varje överföring säkerställs det att organisationens informationspolicy följs. Advenicas ZoneGuard erbjuder en skräddarsydd men enkel lösning baserad på att information allowlistas i en informationspolicy. Lösningen säkerställer att organisationer kan utbyta information mellan säkerhetsdomäner på olika nivåer på ett säkert och korrekt sätt.

### ZoneGuard

ZoneGuard erbjuder en anpassad men enkel informationspolicybaserad lösning för ett säkert informationsutbyte mellan olika säkerhetsdomäner. Som gateway använder den ett tillvägagångssätt som bygger på allowlisting, vidarebefordrar endast mottagen information som överensstämmer med informationspolicyns struktur, format, värden och digitala signaturer. Alla ändringar kräver en digitalt signerad informationspolicy av antingen en IT säkerhetsavdelning eller annan utsedd policygodkännare. ZoneGuard tillhandahåller också styrning av loggar och audit trail - vitala bevis för efterlevnad av policyer och regler.

### Fördelar

- Gör det möjligt för leverantörer att stödja utrustning via remote desk protocol (RDP)
- Förhindrar riskabla, onödiga anslutningar associerade med RDP, såsom skrivare, mikrofoner och högtalare
- Förhindrar obehörig användning
- Förhindrar direkt nätverkskommunikation, vilket förhindrar att virus och ransomware sprids från webbplatsen till leverantören, och vice versa
- Ger fullständig spårbarhet - vem, vad och när
- Kan förlängas med tidsbegränsad eller schemalagd anslutning
- Möjligt att utforma en princip för tvåhandsfattning som gör det möjligt för en intern gatekeeper att bestämma hur och när anslutning är tillåten

Advenica ZoneGuard

© Advenica 2021

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-in-motion 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**

advenica

© Copyright 2021 Advenica AB. All rights reserved. Advenica and the Advenica logo are trademarks of Advenica AB. All registered and unregistered trademarks included in this publication are the sole property of their respective owner. Our policy of continuous development may cause the information and specifications contained herein to change without notice. Doc. no.: 19234 v1.1

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED