Uw ICT-systemen optimaal beveiligd met BoKS

Wat is FoxT BoKS?

BoKS Access Control is een product van de Zweedse firma FoxT, bedoeld voor het centrale beheer van gebruikersauthenticatie en -authorizatie (Role Based Identity Management en Access Control). De naam is een afkorting voor het Zweedse "Behrighet- och KontrollSystem", wat zich laat vertalen als "Legitimatie en controle systeem".

Belangrijke features van het pakket zijn onder andere:

- Centraal beheer van gebruikersaccounts voor servers en desktop systemen.
- Centraal gedefinieerde toegangsregels voor toegang tot servers, desktops en applicaties.
- Het geheel werkt volledig op basis van rollen: RBIM en RBAC.
- Diepgaande auditing en monitoring mogelijkheden, onder andere geschikt voor SOx compliancy.
- Ondersteuning voor de meest voorkomende communicatieprotocollen (Telnet, SSH, FTP, RDP).
- Ondersteuning voor gedelegeerde superuser (root) taken op Unix platformen.
- Integratiemogelijkheden met LDAP en NIS+ directory services.
- Uitstekende schaalbaarheid en redundantie, voor een garandeerbare uptime.

Met behulp van BoKS bepaalt u WIE WANNEER toegang krijgt tot WELKE servers, WAT hij daar mag doen en HOE.

BoKS is een vrijstaande applicatie en vereist geen aanpassingen aan het besturingssysteem van uw servers en desktop systemen.

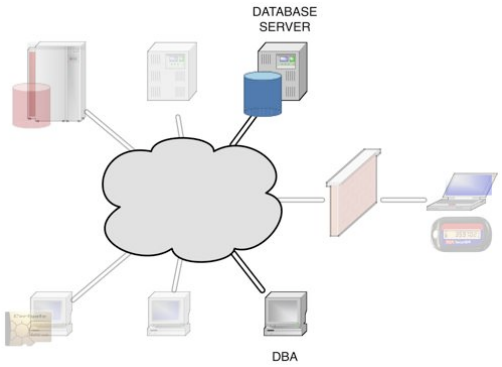
Unixerius is door FoxT gekozen als officiële partner voor de Benelux.

Een praktijkvoorbeeld: Role Based Access Control

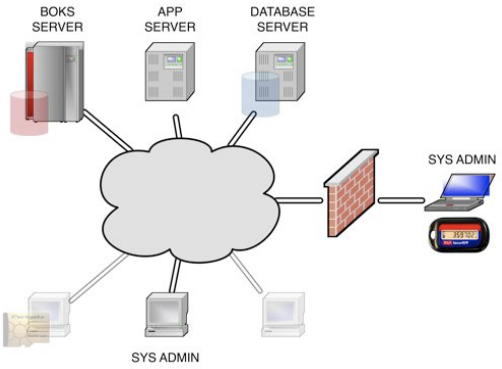
Gebruikers en computersystemen worden in BoKS gegroepeerd op basis van hun functie binnen het netwerk. Elke gebruiker kan beschikken over n of meerdere rollen en elke server maakt deel uit van verscheidene host groepen. De BoKS database is feitelijk een weergave van het organogram van de organisatie, waarbij eenieder een eigen rol binnen het bedrijf vervult.

Als voorbeeld nemen we een netwerk met een BoKS security server, een applicatie server en een database server.

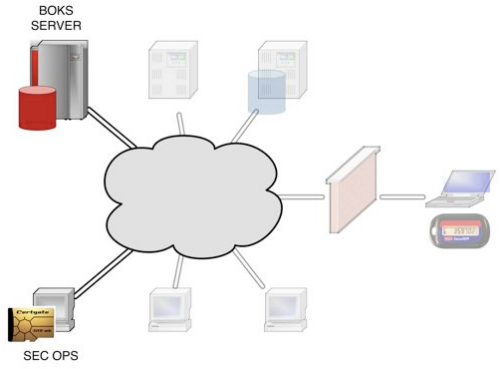
De database beheerders krijgen toegang tot hun eigen werkstations. Daarnaast worden zij toegestaan om met behulp van SSH en SCP op hun Oracle servers in te loggen. Met behulp van de BoKS Oracle plugin worden ook hun gebruikersaccounts in Oracle zelf aangemaakt zodat zij de volledige controle over hun databases krijgen.



De systeembeheerders krijgen vanaf hun werkstations volledige SSH toegang tot alle servers in het netwerk. Omdat zij 24x7 support leveren mogen zij ook via een VPN verbinding met SSH inloggen mits zij zich met een RSA token hebben geauthenticeerd. Om functiescheiding te garanderen krijgen zij geen toegang tot de applicaties en databases die op de servers actief zijn.



Security operations, de eigenlijke gebruikers van BoKS, krijgen SSH toegang tot de BoKS security server. Daarnaast krijgen zij toegang tot de BoKS web interface, mits zij zich identificeren met behulp van een smart card met PKI certificaat.



Key features van BoKS

Centraal beheer van gebruikersaccounts
Gebruikersbeheer hoeft niet langer lokaal te gebeuren. BoKS beheert ook SSH certificaten, secundaire Unix groepen en home directories.

Centraal gedefinieerde toegangsregels
Gebruikers krijgen toegang tot systemen op basis van toegangsregels in de BoKS database die eisen stellen aan zowel het bron- als het doelsysteem, het tijdstip en het gebruikte protocol.

Role based access control
Met behulp van user classes wordt het mogelijk om per afdeling een set toegangsregels te definiëren, waarmee veel tijd en risico's bespaard kunnen worden.

Diepgaande audit logging
Elke authorizatieaanvraag die door BoKS wordt behandeld wordt opgeslagen in de audit logs. Daarnaast is het mogelijk om voor de superuser keystroke logging te activeren.

Real-time monitoring mogelijkheden
De BoKS audit logs worden real-time aangevuld waardoor het mogelijk is om met monitoring tools alarmen te verbinden aan bepaalde situaties.

Ondersteuning voor gebruikelijke protocollen
BoKS ondersteunt authenticatie en authorizatie controle voor de volgende protocollen: login, su, telnet, secure telnet, rlogin, XDM, PC-NFS, rsh en rexec, FTP en SSH. SSH kan verder worden opgesplitst in shell toegang, remote command execution, SCP, SFTP, X11 forwarding) en port forwarding.

Gedelegeerde superuser toegang
Met behulp van de suexec functionaliteit van BoKS wordt het mogelijk om gebruikers zeer gelimiteerde toegang te geven tot superuser accounts.

Integratie met LDAP en NIS+
Indien gewenst is het mogelijk om BoKS samen te laten werken met directory services als LDAP en NIS+.

Redundant uitgevoerde infrastructuur
Het gebruik van meerdere BoKS servers maakt load balancing en een rappe disaster recovery mogelijk.

BoKS werkt met:

solaris
IBM
Microsoft Windows
redhat LINUX
digital
hp
vmware
ORACLE
SAP

Functionaliteit	OpenLDAP	eTrust AC	BoKS AC
Centraal user beheer	✓	✓	✓
Centrale autorisatie configuratie	✓	✓	✓
Role based access control	✖	✓	✓
SSH subsysteem beheer	✖	✖	✓
Monitoring van bestanden	✖	✓	✓
Toegangsbeheer op bestanden	✖	✓	✖
Gedelegeerde superuser toegang	✓	✓	✓
Real-time security monitoring	✓	✓	✓
Diepgaande audit logging	✖	✓	✓
OS blijft ongewijzigd	✓	✖	✓
Gebruikersvriendelijke configuratie	✖	✓	✓
Rapportage tooling	✖	✓	✓
Password vault functionaliteit	✖	✓	✓

Over Unixerius

Unixerius is gespecialiseerd in verscheidene Unix varianten, toegepast in hoogwaardige ICT omgevingen. Onze focus ligt op data security en high availability.

U kunt onze specialisten inhuren voor het *bouwen* van een technische infrastructuur, maar ook voor het *onderhouden* ervan. Onze ervaring stelt ons in staat om u kundig van advies te voorzien en om technische projecten te leiden. Daarnaast geven wij maatwerk-workshops aan uw systeembeheerders. Bijvoorbeeld om hen de basisvaardigheden te leren voor het omgaan met FoxT BoKS, Nagios of SUN Cluster.

Unixerius is FoxT's officiële technology partner voor de Benelux.

www.unixerius.nl

Heeft u vragen? Mail ons op info@unixerius.nl.