Bezpečnostní audit firewallu

Číslo auditu:..... Datum:.....

Adresa:.....
.....
.....

Kontaktní osoba:.....

Telefon:.....

Doporučení:

- Zapnutí automatických aktualizací nebo zavedení pravidelných ručních aktualizací se zápisem do záznamu.
- Zapnout vyžádání hesla do systému po časovém limitu, kdy je firewall v nečinnosti.
- Vypnout nepotřebné služby systému.
- Omezit logování.

1 Řízení bezpečnosti a personální bezpečnost

1.1 Řízení bezpečnosti - bezpečnostní politiky

1.1.1 Jsou dokumentované bezpečnostní politiky schválené managementem?

není dostupné

1.1.2 Obsahují bezpečnostní politiky jména, kdo navrhl bezpečnostní dokument a kdo jej schválil?

není dostupné

1.1.3 Jsou zavedeny prokazatelné seznámení zaměstnanců s bezpečnostními politikami?

není dostupné

1.1.4 Jsou bezpečnostní politiky a nařízení společnosti dostupné zaměstnancům?

není dostupné

1.1.5 Jsou zavedeny nařízení ukládající bezpečnostní kontroly a audity?

není dostupné

1.1.6 Jsou zavedeny nařízení stanovující pravidelné bezpečnostní reporty? (zprávy o bezpečnostních incidentech, risk management)

není dostupné

1.2 Personální bezpečnost

1.2.1 Je zodpovědnost o bezpečnosti pro jednotlivé pracovní funkce definována v popisu práce a v bezpečnostních politikách?

není dostupné

1.2.2 Jsou zaměstnanci prokazatelně proškoleni a trénováni?

není dostupné

1.2.3 Jsou definovány disciplinární zaměstnanců porušující bezpečnostní nařízení?

není dostupné

2 Kontrola firewallu - Fyzická bezpečnost, logický přístup

2.1 Fyzická bezpečnost

2.2.1 Je firewall umístěn v oddělené uzamykatelné místnosti? (např. serverovna)

není dostupné

2.2.2 Je zavedena forma autentifikace při přístupu k firewallu?

není dostupné

2.2.3 Je firewall umístěn v uzamykatelné skříni? (racková skříň)

není dostupné

2.2.4 Je zabezpečena kabeláž proti přímému přístupu? (volně dostupná x chráněná)

není dostupné

2.2.5 Je zavedena forma dohledu nad zařízením? (kamerový systém apod.)

není dostupné

2.2.6 Je využávána záloha napájení? (UPS, generátory)

není dostupné

2.2.7 Je prostředí klimatizováno?

není dostupné

2.2.8 Je veden prokazatelný záznam přístupů k zařízení?

není dostupné

2.2.9 Je přístup k veškeré dokumentaci o firewallu zabezpečen? (uzamykatelná skříň, trezor)

není dostupné

2.2 Logický přístup

2.2.1 Je zavedena politika řízení oprávnění pro definování přístupu ke specifickým zařízením a službám?

není dostupné

2.2.2 Je zavedena politika vytváření a mazání uživatelských účtů?

není dostupné

2.2.3 Je zavedena politika hesel? (změna hesel, síla hesel apod.)

není dostupné

2.2.4 Jsou zavedeny automatické aktualizace?

pouze upozornění na aktualizace

2.2.5 Je zaheslován přístup do BIOSu?

není dostupné

2.2.6 Je zakázáno startování systému z vyměnitelných médií?

není dostupné

2.2.7 Je zaheslován přístup do operačního systému?

ano

2.2.8 Jsou zakázány nezaheslované účty, Guest apod.?

ano

2.2.9 Je zakázáno automatické přihlášení?

ano

2.2.10 Je při nečinnosti po časovém limitu vyžadováno heslo pro přístup do systému?

ne

2.2.11 Jsou datové soubory s hesly zabezpečeny, šifrovány?

ano

2.2.12 Jsou spuštěny jen vyžadované služby?
netstat -an

ne, doporučuje se vypnout nebo zablokovat porty
135 (0.0.0.0),
139 (192.168.20.10, 192.168.30.10, 192.168.40.10)
445 (0.0.0.0)

2.2.13 Pokud je spuštěna vzdálená správa, je použito šifrování? (ssh, HTTPS atd.)

ano

2.2.14 Je při vzdáleném přístupu zakázáno přímé přihlašování administratorského účtu?

ano

2.2.15 Je vyžadována autentizace pro vzdálenou správu?

ano

2.2.16 Nejsou využívána defaultní hesla zařízení?

ano

3 Kontrola pravidel filtrování

Doporučení auditu: Audit pro jeden stavový paketový firewall filtrující provoz pro lokální sítí a DMZ využívající IPv.4.

3.1 Jaký firewall je použit? (HW X SW)

SW

3.2 Na jakém operačním systému firewall běží?

Windows 2003 R2 SP2

3.3 Jaké rozsahy IP adres firewall používá a jak jsou přiděleny síťovým rozhraním a do zón?

192.168.20.10/24 - LAN - Local Area Connection 3
192.168.30.10/24 - WAN - Local Area Connection
192.168.40.10/24 - DMZ - Local Area Connection 2

3.4 Jaké servery poskytují služby vnější síti? (IP adresy, služby)

192.168.40.20/24 – HTTP, HTTPS

192.168.40.30/24 – HTTP, HTTPS, POP3,POP3S, SMTP,SMTPS,IMAP, IMAPS

3.5 Jsou veškeré veřejně dostupné servery v DMZ síti?

ano

3.6 Jsou ostatní PC řádně přiděleny do LAN sítě (sítí)?

ano – 1 LAN – 192.168.20.0/24

3.7 Je spouštění firewallu automatické?

ano

3.8 Je zavedeno správné pořadí pravidel?

- *Anti-spoofing filtr (blokované privátní adresy, interní adresy z vnější sítě),*
- *logování a blokování útoků,*
- *zakazující pravidla,*
- *povolovací pravidla – uživatelská (např. veřejný web server),*
- *povolovací pravidla – správa (např. SNMP),*
- *logování (odladění filtrování, informace o filtrované komunikaci na síti).*

ano

3.9 Je zakázán tzv. source routing?

ano

3.10 Je logování dostatečně omezováno? (počet záznamů za jednotku času)
-m --limit $Nr/$TIME -j LOG

není dostupné

3.11 Jsou defaultní politiky nastaveny na zahazování paketů?
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

ano

3.12 Jsou zakázány příchozí pakety z vnější sítě se zdrojovou adresou vnějšího rozhraní?

ano

3.13 Jsou zakázány příchozí pakety z vnější sítě s privátní zdrojovou adresou (RFC 1918), neroutovatelnou adresou nebo adresou APIPA?

ano

3.14 Je zakázáno broadcast vysílání na jednotlivých rozhraních? Jeli vyžadováno, je blokováno alespoň icmp broadcast vysílání (RFC 2644)?
iptables -A INPUT -i $ANY_IF -m pkttype --pkt-type broadcast -j drop
iptables -A FORWARD -i $ANY_IF -m pkttype --pkt-type broadcast -j drop

ano

3.15 Je zakázáno multicastové vysílání?
iptables -A INPUT -i $ANY_IF -m pkttype --pkt-type multicast -j drop
iptables -A FORWARD -i $ANY_IF -m pkttype --pkt-type multicast -j drop

ano

3.16 Je logován a blokován tzv. SYN-flood na všech rozhraních na vstupu a v tabulce FORWARD? Je zapnut SYN-cookies?

ano

3.17 Jsou logovány a blokovány tzv. Bogus (falešné) pakety na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags SYN, FIN SYN, FIN

kotrola záplav paketů zapnuta, IDS port scan vypnut

3.18 Je logováno a blokováno FIN/URG/PSH skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags ALL FIN, URG, PSH

kotrola záplav paketů zapnuta, IDS port scan vypnut

3.19 Je logováno a blokováno SYN/RST skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags SYN, RST SYN, RST

kotrola záplav paketů zapnuta, IDS port scan vypnut

3.20 Je logováno a blokováno FIN skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags FIN, ACK FIN

kotrola záplav paketů zapnuta, IDS port scan vypnut

3.21 Je logováno a blokováno FIN Stealth skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags ALL FIN

kotrola záplav paketů zapnuta, IDS port scan vypnut

3.22 Je logováno a blokováno Null skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags ALL NONE

kotrola záplav paketů zapnuta, IDS port scan vypnut

3.23 Je logováno a blokováno XMAS skenování na všech rozhraních na vstupu a v tabulce FORWARD?
--tcp-flags FIN, URG, PSH

kotrola záplav paketů zapnuta, IDS port scan vypnut

3.24 Je blokováno UDP skenování na všech rozhraních na vstupu a v tabulce FORWARD?

kotrola záplav UDP paketů zapnuta

3.25 Je povolena komunikace na rozhraní loopback?

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -i lo -j ACCEPT

ano

3.26 a) V případě veřejných adres v DMZ je prováděn NAT pro LAN na externím rozhraní firewallu i na rozhraní DMZ?
iptables -t nat -s $LAN -o $EXT_IF -A POSTROUTING -j MASQUERADE
iptables -t nat -s $LAN -o $DMZ_IF -A POSTROUTING -j MASQUERADE

ano

3.26 b) V případě privátních adres v DMZ je prováděn NAT na externím rozhraní firewallu pro obě sítě ?
iptables -t nat -o $EXT_IF -A POSTROUTING -j MASQUERADE

není dostupné

3.27 Je povolena zpětná komunikace, tj. povolení navázaných spojení?
iptables -A FORWARD -i $EXT_IF -o $LAN_IF -m state --state ESTABLISHED, RELATED
iptables -A FORWARD -i $DMZ_IF -o $LAN_IF -m state --state ESTABLISHED, RELATED
iptables -A INPUT -m state --state ESTABLISHED, RELATED

ano

3.28 Které služby jsou při přístupu na firewall blokovány?
iptables -A INPUT -i $ANY_IF -p $PACKET_TYPE --dport $PORT -j DROP
iptables -A INPUT -p icmp -m icmp --icmp-type $Nr -j DROP

nejsou vyžadovány přímo zakazující pravidla

3.29 Na vstupu jednotlivých rozhraní je povolena komunikace pouze pro požadované služby poskytované firewallem?
iptables -A INPUT -i $ANY_IF -p $PACKET_TYPE --dport $PORT -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type $Nr -j ACCEPT

ano -LAN, DMZ, WAN: RDP(tcp 3389), ping(icmp echo)

3.30 Které služby jsou zakázány z Lan do vnější sítě?
iptables -A FORWARD -i $LAN_IF -o $EXT_IF -p $PACKET_TYPE --dport $port -j DROP
iptables -A FORWARD -i $LAN_IF -o $EXT_IF -p icmp -m icmp --icmp-type $Nr -j DROP

nejsou vyžadovány přímo zakazující pravidla

3.31 Jsou povoleny pouze specifické služby (porty) vnější sítě pro LAN? (připojení na internet)
iptables -A FORWARD -i $LAN_IF -o $EXT_IF -p $PACKET_TYPE --dport $port -j ACCEPT
iptables -A FORWARD -i $LAN_IF -o $EXT_IF -p icmp -m icmp --icmp-type $Nr -j ACCEPT

ano – DNS(udp 53), HTTP(tcp 80),HTTPS(tcp 443), ping(icmp echo)

3.32 Které služby jsou zakázány z Lan do DMZ?
iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p $PACKET_TYPE --dport $port -j

DROP
iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p icmp -m icmp --icmp-type $Nr -j DROP

nejsou vyžadovány přímo zakazující pravidla

3.33 Jsou povoleny pouze požadované služby (porty) poskytované servery v DMZ síti pro LAN?
iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p $PACKET_TYPE -- dport $port -j ACCEPT
iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p icmp -m icmp --icmp-type $Nr -j ACCEPT

ano – omezení na cílový dmz server a cílový port dmz_server – povolené služby 192.168.40.20 - HTTP(tcp 80),HTTPS(tcp 443), ping(icmp echo) 192.168.40.30 - HTTP(tcp 80), HTTPS(tcp 443), SMTP(tcp 25), SMTPS(tcp 465),POP3 (tcp 110), POP3S (tcp 993), IMAP (tcp 143), IMAPS(tcp 995), ping(icmp echo)

3.34 Které služby jsou zakázány z DMZ do Wan?
iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p $PACKET_TYPE --dport $port -j DROP
iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p icmp -m icmp --icmp-type $Nr -j DROP

nejsou vyžadovány přímo zakazující pravidla

3.35 Jsou povoleny pouze požadované služby (porty) vnější sítě pro DMZ? (připojení na internet)
iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p $PACKET_TYPE -- dport $port -j ACCEPT
iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p icmp -m icmp --icmp-type $Nr -j ACCEPT

ano – omezení na zdrojový dmz server a cílový port dmz_server – povolené služby 192.168.40.30 - SMTP(tcp 25), SMTPS(tcp 465)

3.36 a) V případě veřejných adres v DMZ je prováděn forward pro poskytované služby.
iptables -A FORWARD -i $EXT_IF -d $IP_SERVER -p $PACKET_TYPE --dport $PORT -j ACCEPT
iptables -A FORWARD -i $EXT_IF -d $IP_SERVER -p icmp -m icmp --icmp-type $Nr -j ACCEPT

ano – statický NAT, forward omezení na cílový server a cílový port dmz_server – povolené služby 192.168.40.20 - HTTP(tcp 80),HTTPS(tcp 443), ping(icmp echo) 192.168.40.30 - HTTP(tcp 80), HTTPS(tcp 443), SMTP(tcp 25), SMTPS(tcp 465),POP3 (tcp 110), POP3S (tcp 993), IMAP (tcp 143), IMAPS(tcp 995), ping(icmp echo)

3.36 b) V případě privátních adres v DMZ je prováděn překlad adres a forward pro poskytované služby?
iptables -A PREROUTING -d $PUBLIC_IP_DMZSERVER -i $EXT_IF -j DNAT --to-destination $PRIVATE_IP_DMZSERVER

iptables -A FORWARD -i $EXT_IF -d $PRIVATE_IP_DMZSERVER -p $PACKET_TYPE --dport $PORT -j ACCEPT
iptables -A FORWARD -i $EXT_IF -d $PRIVATE_IP_DMZSERVER -p icmp -m icmp --icmp-type $Nr -j ACCEPT

není dostupné

3.37 Je povolena zpětná komunikace pro daný server v DMZ poskytující služby?
iptables -A FORWARD -s $IP_SERVER -p $PACKET_TYPE -m state --state ESTABLISHED, RELATED -j ACCEPT

ano

3.38 Je prováděno logování paketů před konečným zahozením v INPUT, OUTPUT i FORWARD tabulce?

ano

3.39 Dochází ke vzájemné kolizi pravidel?

ne

3.40 Jsou některá pravidla nadbytečná?

ne

4 Kontrola údržby a monitorování

4.1 Kontrola údržby - záznamy, procedury

4.1.1 Jsou vedeny záznamy o haváriích HW a výpadcích firewallu?

není dostupné

4.1.2 Jsou vedeny záznamy o reinstalacích, restartech a obnovách ze záloh?

není dostupné

4.1.3 Jsou vedeny záznamy o provedených zálohách?

není dostupné

4.1.4 Jsou zálohy správně vytvořeny? (zda jsou skutečně vytvořeny při automatických zálohách)

není dostupné

4.1.5 Jsou zálohy pravidelně kontrolovány?

není dostupné

4.1.6 Jsou vytvořeny procedury schvalování pro změny konfigurací firewallu?

není dostupné

4.1.7 Jsou vedeny záznamy změn konfigurací firewallu?

není dostupné

4.1.8 Jsou vedeny záznamy o bezpečnostních incidentech?

není dostupné

4.1.9 Jsou vytvořeny procedury reakcí na bezpečnostní incidenty?

není dostupné

4.2 Monitorování, logování

4.2.1 Je zavedeno monitorování firewallu? (status, bezpečnostní incidenty, zasílání upozornění apod.)

ne

4.2.2 Je prováděno logování firewallu?

ano

4.2.3 Jsou logovány veškeré útoky a užitežné informace firewallu?

ano

4.2.4 Je míra logování přiměřená?

ne – zvážit, zda je nutné logování veškeré komunikace

4.2.5 Jsou logovací soubory zálohovány?

není dostupné

4.2.6 Je prováděna pravidelná kontrola logů?

není dostupné

Jméno auditora:..... Datum:.....

Převzal:..... Datum:.....