# Guía de Seguridad

**Fecha de Publicación:** 15/09/2020
**Fecha de Actualización:** 17/02/2022
**Tema:** Guía de mitigación ante compromiso de una cuenta de correo.

Un problema común que se presenta en los servidores de correo es que se comprometa alguna cuenta de usuario y ésta sea utilizada con el objetivo de envío de correo spam masivo, mensajes de phishing u otro tipo de mensajes maliciosos. A continuación le presentamos el siguiente procedimiento si se encuentra ante un incidente donde su servidor de correo es comprometido y esté enviando correos maliciosos:

1. **Identificar la cuenta comprometida**

   Una de las primeras medidas a tener en cuenta ante un incidente donde un servidor de correo es comprometido y se encuentra enviando email spam, consiste en detectar el origen del problema, esto podría darse en varios escenarios, una de ellas es que el spam se esté enviando desde una cuenta de usuario.

   En este caso se tendría que suspender la cuenta o sencillamente cambiar la contraseña de la cuenta comprometida para evitar que se siga enviando Spam, a su vez comprobar los archivos logs que proveen detalles de las operaciones realizadas sobre el servidor y los eventos ocurridos a modo de bitácora a partir de ellos es posible verificar, en la mayoría de los casos, sí se comprometió el servidor a través de una cuenta de usuario o si otros tipos de fallos fueron explotados.

   Usaremos como ejemplo el servidor de correos Zimbra para encontrar una cuenta comprometida. El siguiente comando mostrará una lista de usuarios que se han autenticado más veces en el periodo de tiempo detallado en el *zimbra.log*.

```
grep sasl_user /var/log/zimbra.log | sed 's/.*sasl_username=//g' | sort | uniq -c |
sort -nr | head
```

   La cuenta comprometida da como resultado que el servidor se use para enviar correos no deseados. Normalmente, si bloquea a un usuario, no debería poder enviar correos electrónicos, pero eso no funcionará si las sesiones smtp ya existen.

2. **Cambio de contraseña**

   Se recomienda tomar las medidas necesarias, entre ellas, bloquear y/o cambiar la contraseña de la cuenta comprometida cuanto antes, eligiendo una contraseña robusta (mínimo 10~12 caracteres, combinación de minúsculas, mayúsculas, números, caracteres especiales, evitar palabras fáciles o comunes, evitar uso de fecha de cumpleaños que puedan ser fácilmente encontradas, etc.)

   **Configurar políticas de contraseña en el servidor Zimbra.**

   Se recomienda la configuración de políticas de contraseña y de control de acceso en los servidores de correo, asegurando la utilización de contraseñas robustas, cambio de contraseñas, y minimizando los intentos fallidos, no solo por cuenta sino también por IP. Las instrucciones específicas varían de

acuerdo a cada software de correo.

En el caso de Zimbra, las políticas de contraseña y de fallos de inicio de sesión se configuran desde el **panel de administración**, de la siguiente manera:

1) Va a "**Configurar**" > "**Clase de servicio**" > "**default**" o la clase que haya establecido (en caso de que lo hubiera personalizado).
2) Seleccionar "**Avanzado**"
3) Valores recomendados:
   A. Tamaño mínimo de la contraseña: 10
   B. Mínimo de caracteres en mayúsculas: 1
   C. Mínimo de caracteres en minúsculas: 1
   D. Mínimo de signos de puntuación: 1
   E. Mínimo de caracteres numéricos: 1
   F. Antigüedad máxima de la contraseña (días): 90
   G. Número mínimo de contraseñas únicas en el registro: 3
   H. Activar bloqueo de inicio de sesión fallido: Tildado
   I. Número de intentos fallidos permitidos para iniciar sesión: 5 *
   J. Tiempo antes de bloquear la cuenta: 1 hora
   K. Período de tiempo dentro del cual deben tener lugar los intentos fallidos de iniciar sesión para bloquear la cuenta: 30 min.

*** Obs.**: Debe encontrarse un balance para este valor, ya que el mismo no contempla los intentos de IPs diferentes. En caso de que activará adicionalmente **fail2ban** o similar, se recomienda aumentar dicho valor, por ejemplo a 10, o personalizarlo de acuerdo a sus necesidades.

### 3. Limpiar cola de correos

La cola de correo es un directorio del servidor que almacena correos que aún no se han entregado por diferentes razones. Cuando el servidor de correo está comprometido y se encuentra enviando mail Spam es importante saber cómo manejar la cola de correos. Si se acumulan demasiados mensajes, su servidor podría dejar de funcionar correctamente, afectado por los mensajes en espera y los que hayan rebotado. Se recomienda eliminar y depurar frecuentemente como medida ante un incidente.

En el caso de Zimbra, por ejemplo, la cola de correo está ubicada en **/var/spool/mqueue**. Las herramientas que el **postfix** proporciona se encuentran dentro de **/opt/zimbra/postfix/sbin**. No solo podrá encontrar las herramientas para el manejo de colas sino también configurar parámetros, crear aliases, etc.

Para verificar la cantidad de mensajes en cola con la herramienta **postqueue**, debe utilizar el parámetro, ***-p.*** Con esto nos mostrará los mensajes que hay en proceso (cola deferred y active):

```
[root@zimbra sbin]# ./postqueue -p
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
1B6FE682F9    22910 Wed Sep  3 17:09:39  MAILER-DAEMON
(connect to mail.member.gocyberlink.com[203.70.119.145]: Connection timed out)
Membership@member.gocyberlink.com
CE801682F8488323 Wed Sep  3 17:09:38  xxxx@xxxxx.com
```

```
(connect to hotamil.com[65.74.135.110]: Connection timed out)
yyyy@hotmail.com
C18C368288    42744 Wed Sep  3 17:09:51  xxxx@xxxxx.com
(connect to hotamil.com[65.74.135.110]: Connection timed out)
yyyyy@hotamil.com
58D796836C   536981 Fri Sep  5 14:22:39  rrrrrr@xxxxx.com
(host mx.poczta.interia.pl[217.74.64.238] said: 450 4.7.1 : Helo command rejected:
Host not found (in reply to RCPT TO command)) hhhhh@fffff.pl
-- 1066 Kbytes in 4 Requests.
```

Con esta herramienta visualizará cuántos mensajes están pendientes de ser procesados y el tamaño de todos ellos. Si por ejemplo, si nota que tiene 125 mensajes por procesar y 450Mb de correo esto le dará indicio de lo que está pasando.

**Para borrar la cola de correos:**

Inicie el sistema como usuario **root y** ejecute el siguiente comando.

```
#/opt/zimbra/postfix/sbin/postsuper -d ALL deferred
```

Este comando es usado para eliminar todos los correos diferidos por rebote, generados por alguna cuenta comprometida o algún ataque de suplantación de identidad (mail spoofing). Se recomienda siempre revisar **/var/log/mail.log** para confirmar qué cuenta o IP es la causante y podría poner dicha IP dentro de un filtro de lista negra como "**fail2ban**" y/o bloquear dicha IP desde el firewall.

Para borrar todos los correos encolados en Zimbra MTA (postfix) en un servidor de linux, ejecute el siguiente comando como usuario root:

```
root@localhost#/opt/zimbra/postfix/sbin/postsuper-d ALL
```

**4. Revisar Listas Negras de SPAM**

Las listas negras de spam también conocidas como SPAM Blacklist tienen como misión identificar direcciones IP que han llevado a cabo prácticas de spam a través de correo electrónico. Su objetivo es

informar a los servidores de correo electrónico para que éstos rechacen los mensajes que provengan de esas direcciones o los marquen como SPAM.

Es importante asegurar que nuestra IP no aparezca en ninguna de estas listas, de lo contrario, los correos enviados por los usuarios del servidor de correo que se administra no llegarán a destino. Si la IP de su servidor de correo fue incluida dentro de una de esas listas es importante revisar las condiciones de la lista para saber qué pasos tomar para salir de la misma. En muchos casos, la lista elimina automáticamente la IP después de un cierto tiempo.

En algunos casos, el responsable de la IP debe contactar a los administradores de la lista. La mayoría de las listas negras exigen que sea el propio administrador de la IP del servidor de correo quien realice la petición, comprobando que la petición se esté enviando desde el propio servidor de correo o del mismo bloque de IP, por lo que no aceptan que se delegue a un tercero ese proceso.
Le recomendamos:

- Seguir las instrucciones para salir de cada lista negra, ya que cada lista tiene su propio procedimiento y mecanismo. Algunos de ellos son pagos pero todos tienen fecha de expiración y van de 7 a 30 días.
- Antes de pedir salir de una lista negra debe estar lo más seguro posible que incidentes similares no se repitan prontamente porque si vuelven a ingresar a lista las penalizaciones suelen ser más severas, pueden agregar varias semanas de pertenencia a la lista negra.

**Listas Negras más utilizadas:**

- Spamhaus, https://www.spamhaus.org/
- Abuseat(CBL), https://www.abuseat.org/
- Sorbs, http://www.sorbs.net/
- Uceprotect, http://www.uceprotect.net/
- Lashback, https://blacklist.lashback.com/
- Spamcop, https://www.spamcop.net/
- Barracuda, https://www.barracuda.com/

## 5. Activar control Rate Limit de correo

Si una cuenta está comprometida, es común que se empiece a enviar muchos correos en un lapso de tiempo corto, para prevenir esto se puede limitar la cantidad de correos que se envía en un periodo de tiempo por usuario , por ej: no más de 10 mensajes en una hora por usuario, no más de 50 correos por día por usuario, etc. Para hacer esto se usa la configuración **rate limit.** La mayoría de los servidores de correo traen esta funcionalidad, la cual debe ser configurada por el administrador.

Si bien, esto no evitará que la cuenta se comprometa y tampoco evitará completamente el envío de correos spam, reducirá el impacto ya que el volumen de spam generado se bloqueará antes de que el envío sea demasiado elevado.

A continuación damos ejemplo de cómo configurar **rate limit** en **Zimbra:**

Para habilitar **rate limit,** bastaría con editar el fichero de configuración de postfix,

```
shell> vi /opt/zimbra/postfix/conf/main.cf
```

Y agregar:

```
smtpd_client_message_rate_limit = 10
anvil_rate_time_unit = 60
```

Tras ello, reiniciar el servidor MTA

```
shell> zmmtactl restart
```

Con ello conseguimos limitar a 10 la cantidad de correo que sale de Zimbra por usuario, también existe la posibilidad de aplicar los cambios sin reiniciar el servicio, ejecutando los siguientes comandos:

```
shell> postconf -e anvil_rate_time_unit=60s
shell> postconf -e smtpd_client_message_rate_limit=10
```

6. **Implementar Alertas**

Un sistema de monitorización correctamente parametrizado brinda a los administradores información relevante sobre la situación de los servicios, que a su vez pueden utilizar dicha información para tomar acciones reactivas; solucionando problemas complejos antes de que provoquen problemas de disponibilidad y/o capacidad, y también tomar acciones proactivas; que mediante el estudio de tendencias y eventos promuevan cambios en la infraestructura con el fin de evitar futuros fallos o explotación de los mismos.

Habilitar las alertas o notificaciones para cuando estos rate limit sean superados por un usuario, de modo a que pueda detectar cuanto antes el compromiso de una determinada cuenta.

Una posible herramienta para la monitorización es **Nagios**, la cual se integra a Zimbra. **Nagios** es un sistema de monitorización de redes ampliamente utilizado desde su lanzamiento en 1999, es de código abierto y vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...). **Para configurar Nagios con Zimbra** puede dirigirse al siguiente enlace: https://wiki.zimbra.com/wiki/Monitoring_Zimbra_Collaboration_Nagios.

7. **Implementar un Security Gateway**

Los agentes de transferencia de mensajes (MTA) están siendo sustituidos por dispositivos GATEWAY de correo electrónico a fin de reforzar la seguridad del sistema. Las puertas de enlace de correo electrónico seguro son puertas de enlace diseñadas para filtrar el tráfico de correo.

Se implementa esta solución para combatir ataques como phishing, ataques transmitidos por correo electrónico, virus, malwares y más ataques que pueden filtrarse por una puerta de enlace de correo electrónico, pero también puede evitar la fuga de información por parte de miembros infieles de la organización.

Un **Email Secure Gateways (ESG**) puede estar disponible como un servicio en la nube, como dispositivo virtual, localmente en el servidor de correo y hay también soluciones de software y hardware.

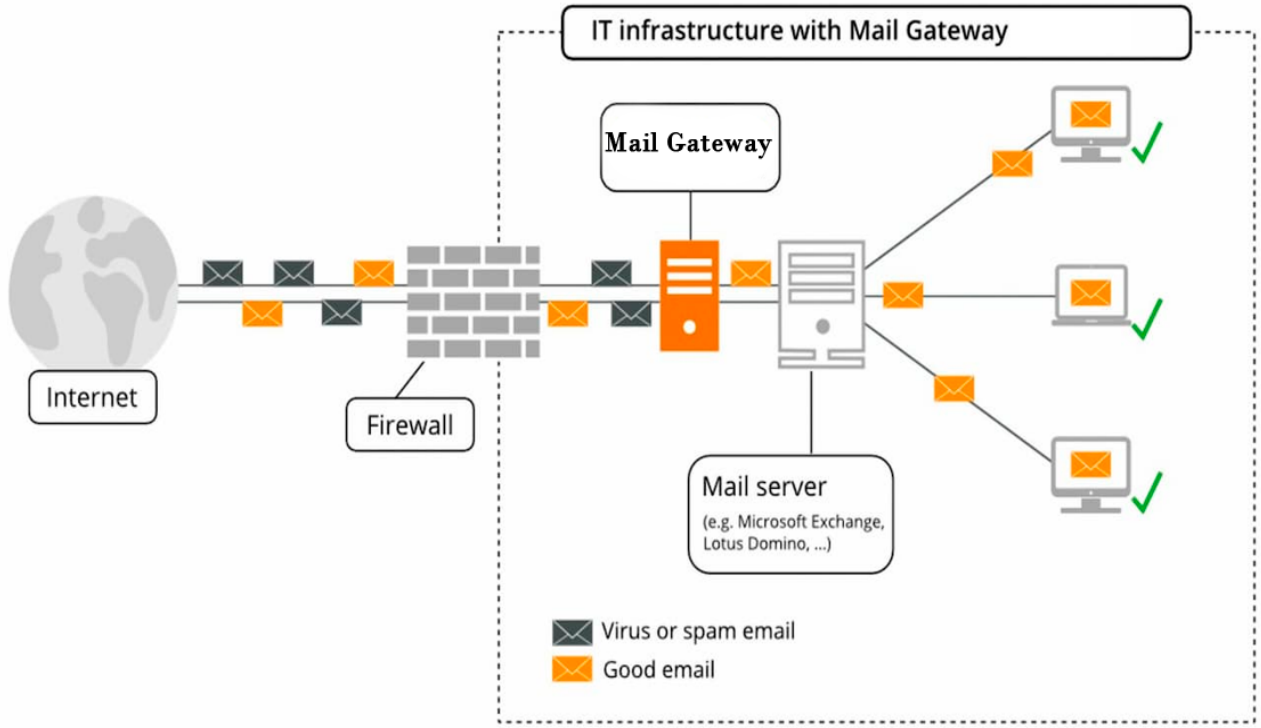
A diferencia de las soluciones **Anti-Spam**, los **ESG** proporcionan una gestión avanzada del tráfico de mensajes mediante herramientas que refuerzan las políticas, filtran contenidos y ofrecen informes detallados.

**Diferencias entre un Anti-Spam y Email Security Gateway.**

Las soluciones **Anti-Spam** poseen funciones específicas de protección y por ende más limitadas, también podría afectar el rendimiento del servidor, así mismo si se instala y configura en un servidor externo, en modo pasarela, es mucho más compleja de mantener y configurar.

En cuanto al **Email Security Gateway** como está instalado en paralelo con el servidor de correo por ende no utiliza los recursos de la misma garantizando el buen funcionamiento y brindando más funciones. Al configurarse en un servidor externo, en modo pasarela, es menos complejo que los Anti-Spam y de más

sencilla implementación. Otra función característica es su protección contra software malicioso aplicando técnicas de un antivirus. Protege al servidor de correos antes que lleguen las conexiones, a la vez ofrece protección contra phishing, URL maliciosas, ingeniería social, spam, entre otros.




**Algunas soluciones Email Security Gateway:**
Existen muchas empresas que ofrecen soluciones de ESG **comerciales** entre ellas:

1. MDaemon Email Server
2. Proofpoint
3. Barracuda Email Security Gateway
4. mimecast

También existen algunas opciones **gratuitas**, como por ejemplo:

1. **Proxmox Mail Gateway** https://www.proxmox.com/en/proxmox-mail-gateway
   Guia de instalación y configuración: https://www.proxmox.com/en/proxmox-mail-gateway

2. **MailScanner:** https://github.com/MailScanner/v5/tree/master/builds
   Guia de instalación y configuración: https://www.mailscanner.info/MailScanner.conf.index.html

3. **Hermes Secure Email Gateway:** https://github.com/deeztek/Hermes-Secure-Email-Gateway
   Guia de instalación y configuración:
   http://www.caroligualada.es/Documentos/Guia%20rapida%20LC1.pdf

## 8. Backup de Logs

Se recomienda implementar políticas de backup de logs y almacenarlos por al menos **6 meses**. Los logs registran actividades del servidor de correo y errores en una combinación de registros del sistema a través del servicio **syslog**, así como registros específicos de su servidor de correo en el sistema de archivos local.

A continuación damos unos ejemplos de registros logs pertenecientes a **Zimbra**. Los registros que se describen a continuación son los registros principales que se utilizan para el análisis y la resolución de problemas:

Los **registros locales** que contienen actividad de Zimbra están en el directorio `/opt/zimbra/log`:

- **audit.log**. Este registro contiene actividad de autenticación de usuarios y administradores y fallas de inicio de sesión. Además, registra la actividad del administrador para poder realizar un seguimiento de los cambios de configuración.

- **clamd.log**. Este registro contiene actividad de la aplicación antivirus clamd.

- **freshclam.log**. Este registro contiene información de registro relacionada con la actualización de las definiciones de virus del **clamd**.

- **logger_myslow.log**. Este registro de consulta lenta consta de todas las instrucciones SQL que tardaron más de X segundos en ejecutarse. El valor de X se puede definir en **long_query_time** ubicado en **/opt/zimbra/my.logger.cnf**.

- **myslow.log**. Este registro de consulta lenta consta de todas las sentencias SQL del servidor de buzones de correo que tardaron más de dos segundos en ejecutarse. Si desea modificar el umbral de tiempo para registrar las consultas SQL, puede modificar la configuración **long_query_time** la cual se define en **/opt/zimbra/my.cnf.**

- **spamtrain.log**. Este registro contiene resultados de **zmtrainsa** durante ejecuciones programadas regularmente desde el cron.

- **sync.log**. Este registro contiene información sobre las operaciones de sincronización móvil de ZCS.

**Otros registros incluyen:**

- `/opt/zimbra/jetty/logs/`. Aquí es donde se registra la actividad específica de Jetty.

- `/opt/zimbra/db/data.<nombrehost>.err`. Este es el registro de errores de la base de datos del almacén de mensajes.

- `/opt/zimbra/logger/db/data.<nombrehost>.err`. Este es el registro de errores de la base de datos del registrador.

**Actividad de ZCS registrada en el syslog del sistema.**

- `/var/log/zimbra.log`. El syslog de Zimbra detalla las actividades de Zimbra MTA (Postfix, amavisd, antispam, antivirus), Logger, Authentication (cyrus-sasl) y Directory (OpenLDAP). Por defecto, la actividad LDAP se registra en Zimbra.log.

**Utilización de Bash scripts**

Puede utilizar un scripts para automatizar el proceso de backups de logs, aquí un ejemplo:

```
#/opt/zimbra/postfix/sbin/postsuper -d ALL deferred
#!/bin/sh
LOG=/var/log/backup.log
FECHA="$(date +"%d-%m-%Y")"
HORA="$(date +"%H:%M:%S")"
DIRBCK=/media/BACKUPSO/Linux
MAILINFO=tu@mail.com
SERVER=$(hostname)
echo >> $LOG
echo "--------------------" >> $LOG
echo "COPIA DE SEGURIDAD " >> $LOG
echo "Fecha:" $FECHA >> $LOG
echo "Hora:" $HORA >> $LOG
echo "Servidor:" $SERVER >> $LOG
echo "--------------------" >> $LOG
tar cvzpf /root/${SERVER}${FECHA}.tgz --same-owner
--exclude=/root/${SERVER}${FECHA}.tgz --exclude=${LOG} --exclude=/proc/*
--exclude=/media/* --exclude=/dev/*  --exclude=/mnt/* --exclude=/sys/*
--exclude=/tmp/* / >> $LOG
rsync -a --human-readable --stats /root/${SERVER}${FECHA}.tgz $DIRBCK >> $LOG
rm /root/${SERVER}${FECHA}.tgz
echo "------------------------------" >> $LOG
echo "COPIA DE SEGURIDAD FINALIZADA " >> $LOG
echo "Fecha:" $FECHA >> $LOG
echo "Hora:" $HORA >> $LOG
echo "Servidor:" $SERVER >> $LOG
echo "------------------------------" >> $LOG
mailx -s "BACKUP: Log de la copia de seguridad" $MAILINFO < $LOG
rm $LOG
Capacitación
```

Para mayor detalle sobre logs del servidor Zimbra  siga el siguiente enlace:

http://docs.zimbra.com/docs/os/6.0.10/administration_guide/9_Monitoring.12.08.html

## 9. Capacitación del usuario contra phishing

Es recomendable realizar capacitaciones y campañas de concienciación periódicas para sus usuarios, de manera a que éstos no caigan en phishing y/o correos fraudulentos.

Considerando que el usuario siempre será la última línea de defensa, cabe destacar la importancia de incluir un plan de capacitación institucional para adiestrar al personal activo y a los nuevos incorporados, se recomienda realizarlo permanentemente siguiendo un cronograma de capacitación basados en diversas técnicas y mecanismos como cursos, charlas, ejercicios, material audiovisual y campañas que deberán estar contemplado en el plan institucional.

Desde el MITIC se ofrecen servicios de concienciación y capacitación para usuarios de instituciones públicas. Para más información sobre el servicio, puede leer el siguiente link:
https://www.cert.gov.py/index.php/servicios/ciberejercicios-simulacro-de-ciberataque

**Fuentes:**

http://noc.usac.edu.gt/blog/?p=478
https://vdocuments.es/ver-colas-de-correo-en-zimbra-55b34a0f5654b.html
http://www.idz.vn/2016/06/zimbra-tips-how-to-configure-rate-limit.html
https://www.boscolopez.com/script-realizar-copia-de-seguridad/