Paso 1:

Hoy me llegó un correo que parecía súper legítimo, Era supuestamente de facebook, por eso me pedían que hiciera clic en un enlace para verificar mi cuenta o algo así, porque había 'actividad sospechosa'. ¡Casi caigo! El diseño era idéntico y el mensaje parecía urgente.

Menos mal que algo me hizo dudar en el último momento. No sé, quizás la forma en que me pedían los datos o que el enlace parecía un poco raro. Al final, resultó ser un ataque de phishing simulado de un atacante. Menos mal Imagínense si hubiera metido mi contraseña o los datos de mi tarjeta. Qué susto Pero bueno, supongo que así se aprende a estar más atento a estas cosas.

Después de ese correo falso, si me llega uno real parecido, no hago clic en nada, no respondo con datos y verificar directamente con la fuente oficial (web o teléfono conocido). También reviso bien los detalles del correo (remitente, errores, urgencia). Y si dudo, lo reportó Estaré mucho más atento

Paso 2:

Ahora, me toca meterme en los logs para ver qué pasó. Primero, los del servidor de correo, ¿no? Ahí tenemos que buscar si alguien intentó entrar a lo bruto a alguna cuenta, si alguien raro se metió desde China, o si de repente salieron miles de correos sospechosos. También ver si alguien abrió algún archivo raro que llegó por ahí o si cambiaron alguna configuración sin permiso.

Luego, a los logs de la base de datos. Ahí tenemos que ver si alguien se conectó desde una IP que no conocemos, si hicieron consultas raras que no son normales, si cerraron o cambiaron un montón de datos de golpe, o si crearon usuarios nuevos que no deberían estar ahí.

Y claro, los logs de seguridad, esos son clave Tenemos que revisar todas las alertas del firewall, del antivirus, del detector de intrusos, cualquier cosa que haya saltado. Si alguien intentó entrar y lo bloquearon, sí detectaron un virus, o si alguien intentó meterse donde no debía.

Ahora, para encontrar la aguja en el pajar de todos esos logs, toca analizar la actividad. Ver si hay picos raros de actividad a ciertas horas, si algo está pasando demasiado seguido, o si vemos eventos raros que ocurren al mismo tiempo en diferentes sistemas. Por ejemplo, alguien entra al correo y justo después hay actividad sospechosa en la base de datos.

Para esto, podemos usar varias herramientas. Desde el simple buscar en los archivos de texto, hasta programas más potentes como Splunk o ELK, que nos ayudan a ver todo de forma más organizada y a encontrar patrones. También podemos hacer scripts rápidos en Python o algo así para buscar cosas específicas. ¡Toca ponerse el sombrero de detective digital!"

Paso 3:

ok vimos cosas raras en los logs. Ahora toca ver el alcance: aislar los equipos sospechosos de la red y guardar una copia de cómo están. Avisar a los importantes y ver a qué otros equipos estaban conectados. Si son equipos clave para la empresa, alarma

Luego, ver el impacto: ¿qué tan caído está? ¿Se cambió información? ¿Se robaron datos importantes y a cuánta gente afecta?

Al final, necesitamos saber cuántos equipos están mal, cuáles son, cómo se conectan y qué tanto daño hicieron o pudieron hacer. Así sabremos qué tan grave es la cosa.

Paso 4:

Después de ver el desastre en los logs, lo primero es aislar los sistemas que creemos que están comprometidos, desconectarlos de la red sin pensarlo Luego, mientras tanto, correr a actualizar todos los sistemas con los últimos parches de seguridad. Y cambiar inmediatamente todas las contraseñas importantes, sobre todo las de acceso a cosas críticas.

Para volver a la normalidad, lo más seguro es restaurar todo desde las copias de seguridad limpias que tengamos. Pero ojo, después de hacerlo, hay que monitorear los sistemas para asegurarnos de que todo esté bien y que el atacante no haya dejado ninguna sorpresa. Y cuando todo pase, sentarnos a analizar detalladamente lo ocurrido, cómo entraron y qué podemos hacer para que no vuelva a pasar jamás.

Y claro, a todo esto, hay que contarle a la gente importante qué pasó, qué estamos haciendo y qué va a pasar. es lo mejor para que todos estén en la misma conciencia de la situación.