Integrantes:

- Angie Daniela Ruiz Alfonso
- Angi Paola Jiménez Pira
- Juan Sebastián Díaz

Fecha: 22 agosto 2020

# Taller gestión de riesgos

**Parte 1:** Defina ampliamente los conceptos mencionados a continuación:

1. **Activo:** Se refiere a algo tangible o intangible, que aporta valor al negocio. Incluye personas, información, infraestructura, finanzas y reputación. Pueden ser sistemas de información, servidores, información guardada en las bases de datos, redes de comunicación.

2. **Amenaza:** Algo que es capaz de actuar en contra a la infraestructura o a un activo de la empresa, resultando en pérdidas y en daños.

3. **Riesgo:** Es la combinación de probabilidad de un evento y su impacto o consecuencia. Los riesgos son mitigados a través del uso de controles, salvaguardas y contramedidas. Para medir el riesgo, se utiliza la siguiente fórmula:

   Riesgo = probabilidad * impacto

4. **Vulnerabilidad:** Una debilidad en el diseño, implementación, operacional, o de control interno de un proceso que puede exponer el sistema a amenazas adversas desde eventos peligrosos.

5. **Vector de ataque:** Es el camino o patrón usado para atacar y ganar acceso al activo objetivo. Hay dos tipos de vectores: de ingreso y de egreso, también conocido como filtración de datos.

6. **Exploit:** Es un programa o código que se aprovecha de un agujero de seguridad **o** vulnerabilidad en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio. No se puede considerar como un malware, sino que actúa como llave para que los malware puedan ingresar al sistema.

**Parte 2:** Utilizando el ataque elegido como tarea, identifique y explique los elementos del punto anterior, ¿cuál fue el Activo afectado?, cual fue la amenaza presente?, ¿Cuál fue el Riesgo materializado?, ¿se tenía alguna Vulnerabilidad que permitió el ataque?, ¿cuál Vector de ataque?, ¿cuál su el Exploit utilizado?,

Zoom es una plataforma usada por empresas, instituciones educativas y otras organizaciones que buscan alternativas para mantenerse en contacto durante la pandemia del coronavirus. Esta plataforma ha sufrido ciber ataques, se encontraron más de 500 mil registros de cuentas de usuarios Zoom a la venta en la web oscura, entre esos datos se encontraron credenciales pertenecientes a instituciones educativas y compañías de alto perfil como Citibank.

- **Activo afectado**
  En este ataque se vio afectada información privada de la plataforma.

- **Amenaza**
  Ciber criminales

- **Riesgo materializado**
  Se hizo pública información privada de la plataforma y esto tuvo como consecuencia el uso malicioso de estos datos, lo que afectó a clientes Zoom ya que hackers o trolls ingresaron aleatoriamente a llamadas de **Zoom** y publicaron material gráfico o contenido ofensivo, también ingresaron a reuniones empresariales de donde obtuvieron información privada de las empresas; todo esto condujo a una baja en la reputación de la plataforma.

- **Vulnerabilidad que permitió el ataque**
  Después de recibir el ataque, los programadores de la empresa identificaron que tenían Referencias Directas a Objetos de manera insegura, de manera que cualquiera podría acceder a los números de las llamadas personales y también las claves para acceder a las reuniones, así mismo podían manipular la información de la reunión a su gusto.

- **Vector de ataque**
  Se uso el mecanismo de relleno de credenciales o fuerza bruta.

- **Exploit**
  Se usó un Exploit de Ejecución de Código Remoto (RCE), de manera que podían hacer los ataques sin necesidad de realizar otras medidas anteriores. Después de acceder, los hackers podían hacer uso de la máquina de la víctima. Para esto se usó un Exploit de día 0 y otros bugs que la aplicación contiene.

**Parte 3:** Teniendo en cuenta los elementos identificados en el punto anterior, determine el nivel de riesgo al que la empresa se veía expuesto siguiente la siguiente tabla de clasificación del riesgo.

Table 1: Risk Scoring Legend

| Risk Rating Matrix | | Impact | | |
|---|---|---|---|---|
| | | Low | Medium | High |
| Likelihood | Low | L | M | M |
| | Medium | M | M | H |
| | High | M | H | C |

***Likelihood**: Probability of occurrence of the risk event due to gaps identified.*

***Impact** of the risk events in the form of regulatory, operational, legal, financial or reputational consequences for Halliburton.*

| Risk Summary | | | |
|---|---|---|---|
| **Assessment Security Domains** | **Likelihood** | **Impact** | **Overall Risk** |
| **Robo de credenciales o información sensible** | **H** | **H** | **H** |
| **Acceso no autorizado a reuniones privadas** | **H** | **M** | **H** |
| **Publicación de contnido inapropiado o con virus** | **H** | **H** | **H** |

a. **Justificación de Probabilidad**:

Robo de credenciales o información sensible: Alta, porque con la situación actual de la pandemia, trajo consigo como objetivo las plataformas de

comunicación o acceso remoto, de las cuales los cibercriminales buscan aprovecharse para obtener información valiosa.

Acceso no autorizado a reuniones privadas: Alta, porque con la situación actual de la pandemia, trajo consigo como objetivo las plataformas de comunicación o acceso remoto, de las cuales los cibercriminales buscan aprovecharse para obtener información valiosa o causar de una empresa u organización.

Publicación de contenido inapropiado o con virus: Alta, porque con la situación actual de la pandemia, trajo consigo como objetivo las plataformas de comunicación o acceso remoto, de las cuales los cibercriminales buscan generar malestar en los ambientes de clase o reuniones exponiendo a contenido explícito a los menores.

b. **Justificación Impacto**:

Robo de credenciales o información sensible : Alto, porque se puede robar información importante de los usuarios, en donde pueden tener almacenados datos relacionados con cuentas bancarias, información confidencial personal o de una empresa.

Acceso no autorizado a reuniones privadas: Medio, ya que las personas no usan adecuadamente las herramientas de configuración del aplicativo para sus reuniones, lo cual compromete el contenido tratado en ellas.

Publicación de contenido inapropiado o con virus: Alto, al exponerse posiblemente a menores de edad compromete el impacto del ataque.

**Parte 4:** Teniendo en cuenta los puntos anteriores, proponga un control apropiado para mitigar el riesgo, y realice nuevamente la evaluación del riesgo utilizando las tablas descritas en el punto anterior.

- La propuesta de control es que Zoom como plataforma exija a los usuarios creación de cuentas con credenciales más robustas (contraseñas con alta seguridad), ya que actualmente es posible ingresar a las reuniones teniendo sólo el número o link de éstas. Por otro lado, por parte de los usuarios, sería realizar capacitaciones dependiendo del tipo de organización, rol, o sobre qué contenido e información van a difundir/manejar por medio de la plataforma.

Table 1: Risk Scoring Legend

| Risk Rating Matrix | | Impact | | |
|---|---|---|---|---|
| Risk Rating Matrix | | Low | Medium | High |
| Likelihood | Low | L | M | M |
| | Medium | M | M | H |
| | High | M | H | C |

***Likelihood**: Probability of occurrence of the risk event due to gaps identified.*

***Impact** of the risk events in the form of regulatory, operational, legal, financial or reputational consequences for Halliburton.*

| Risk Summary |
|---|

| Assessment Security Domains | Likelihood | Impact | Overall Risk |
|---|---|---|---|
| **Robo de credenciales o información sensible** | **M** | **H** | **H** |
| **Acceso no autorizado a reuniones privadas** | **L** | **M** | **H** |
| **Publicación de contnido inapropiado o con virus** | **C** | **H** | **H** |

a. **Justificación de Probabilidad:**

Robo de credenciales o información sensible: Medio, porque con las medidas tomadas por la plataforma, las claves serán más seguras, pero esto no implica que no exista riesgo de intento de robo y por lo visto este es el mecanismo más común de ataque para el robo de credenciales, y fue el usado anteriormente. Las capacitaciones cubren el eslabón más débil de la comunidad porque son los usuarios los que también pueden ponerse en un riesgo aún más alto del que ya existe con estos ataques vistos anteriormente, por no saber sobre el riesgo o conocer bien el mecanismo de uso debido de la aplicación dependiendo el rol de participación en la plataforma, además del rol en la empresa u organización.

Acceso no autorizado a reuniones privadas: Bajo, porque con las medidas tomadas por la plataforma para las reuniones será mucho más seguro el ingreso y las probabilidades de ingreso indebido serán bajas, pero el riesgo de ataque por algún otro medio que no esté cubierto sigue presente.

Publicación de contenido inapropiado o con virus: Teniendo en cuenta lo de las claves más seguras, las capacitaciones al personal que usará la plataforma y el control aplicado sobre las reuniones, esta combinación de medidas tomadas hace que este riesgo esté controlado, pero no elimina el hecho de que los ataques se dejen de hacer y no exista más la amenaza.

**b. Justificación Impacto**:

Robo de credenciales o información sensible: Alto, porque se puede robar información importante de los usuarios, en donde pueden tener almacenados datos relacionados con cuentas bancarias, información confidencial personal o de una empresa.

Acceso no autorizado a reuniones privadas: Medio, ya que las personas no usan adecuadamente las herramientas de configuración del aplicativo para sus reuniones, lo cual compromete el contenido tratado en ellas.

Publicación de contenido inapropiado o con virus: Alto, al exponerse posiblemente a menores de edad compromete el impacto del ataque.