

Más Allá del "Me Hackearon, Fortaleciendo la Confianza en la Era Digital"

Autor: Gilberto Vicente

Durante una reciente conferencia sobre innovación digital, me aventuré a hacer una pregunta al selecto grupo de líderes empresariales presentes: ¿Han escuchado a algún colega o socio decir "me hackearon"? ... Mi objetivo, aunque un poco audaz e inocente 😊, era introducir la conversación sobre el valor que juega el individuo, como principio y fin, en la CiberSeguridad. Para mi sorpresa, no solo muchos levantaron la mano, sino que algunos rostros reflejaron una familiaridad incómoda con el tema.

Ahora, permítanme aclarar que mi intención nunca fue colocar a nadie en el *spotlight*. Mi meta es, y siempre ha sido, subrayar la relevancia de la seguridad digital y cómo, en el *rush* de la vida empresarial, a menudo pasamos por alto nuestra contribución al problema.

Pensemos en cualquier foro o charla contemporánea y seguro hemos escuchado sobre directivos que han vivido invasiones en sus redes sociales, robo de identidad o alertas de seguridad sobre datos corporativos comprometidos. Estas situaciones, más allá de ser anécdotas, revelan una preocupación latente en nuestro entorno de negocios. Pero, ¿qué esconde esta exclamación, tan común y, al mismo tiempo, tan reveladora?

La Confesión "Digital"

Resulta curioso cómo, ante situaciones de crisis digital, el instinto humano nos lleva a buscar un culpable externo. ¿Es acaso un pretexto moderno y convincente?, cuando nos enfrentamos al espejo de la vulnerabilidad, encontrar un adversario invisible es sin duda más cómodo que admitir fallas propias.

Por duro que parezca para aquellos de nosotros inmersos en la gestión de riesgos digitales (aka CiberSeguridad), para muchas personas expresar un "fui hackeado" representa un respiro temporal. Pero aquí está el meollo del asunto: si bien es cierto que existen amenazas complejas y endémicas en el ciberespacio, lo cierto es que muchos de estos incidentes nacen de lapsos y decisiones propias que dejan la puerta abierta a estos intrusos.

Diversos informes de analistas indican que un asombroso 80% de las afectaciones de seguridad se deben a contraseñas débiles o comprometidas. Pongámoslo en perspectiva: para una corporación con muchos "usuarios" (empleados, socios, bots, etc.) y además empoderados en el uso de tecnología, esto representa un sinfín de potenciales puntos de entrada para actores malintencionados.

Confianza y Reputación en la Balanza Digital

Cuando pronunciamos "me hackearon", más allá de evocar la imagen de un hacker en una habitación oscura, **estamos realmente subrayando nuestra vulnerabilidad en este mundo digital interconectado**. Este grito es un eco de cómo nuestra reputación, construida tras años de esfuerzo, puede ser sacudida por un solo evento. Las ondas de choque no solo nos afectan a nosotros, sino que repercuten en la confianza de nuestros colegas, socios y *stakeholders*. En el mundo de los negocios, la confianza es nuestro activo más valioso y, una vez quebrantada, su reconstrucción requiere tiempo, paciencia y acción.

Para organizaciones de cualquier giro y tamaño, un desliz puede traducirse en la fuga de clientes, litigios y un estigma en su reputación. Un dato para reflexionar: el 85% de los consumidores dudaría en reanudar transacciones con una firma que haya sufrido problemas de seguridad.

Vigilancia Activa e Higiene Digital: Fortalezas en el Ciberespacio

Visualiza el ciberespacio como una gran ciudad en constante evolución. Atravesarla, en términos que nos resonarán a muchos, demanda una postura de "Cero Confianza" o, si prefieren un término más explícito, una postura de "Paranoia Responsable" =P. Se trata de movernos con la certeza de que los riesgos están siempre presentes y que eventualmente nos pegaran por lo que necesitamos prepararnos responsablemente.

Para blindarnos en esta selva digital rodeada de amenazas endémicas, algunas medidas indispensables son:

1. Campañas Educativas: En un ecosistema digital en constante cambio, la formación y sensibilización son cruciales para enfrentar sus desafíos con eficacia
2. Contraseñas Robustas: Los atacantes usualmente no hackean, se loguean. Utiliza un administrador de contraseñas para guardar y generar claves seguras. Considera adoptar soluciones 'password-less' para eliminar contraseñas por completo. Proteger tus accesos es tan vital como cerrar la puerta de tu casa.
3. Verificación Dual: Activa la autenticación de factor múltiple para una capa extra de seguridad. Es como tener dos llaves para una misma puerta. Tu información vale la pena ese paso adicional.
4. Actualizaciones Periódicas: Más allá de nuevas funcionalidades, las actualizaciones corrigen vulnerabilidades conocidas.
5. Aplica el principio "Confianza Cero": desconfía siempre y valida constantemente. Otorga accesos con el mínimo privilegio necesario. Anticipa, y prepárate para responder a amenazas que eventualmente serán exitosas.

Adherirse a las directrices de seguridad es equivalente a cerrar bien la puerta al salir. Adoptando una mentalidad de "Paranoia Responsable" y fortaleciendo nuestra higiene digital, estaremos en posición de aprovechar al máximo el mundo digital.

El mundo digital es un terreno fértil de oportunidades, pero también de amenazas. La próxima vez que te sientas tentado a expresar "me hackearon", haz una pausa. Reflexiona sobre tus hábitos digitales y considera si has tomado todas las precauciones necesarias. En esta era, la confianza es un bien precioso y la inocencia no nos exime de culpa ante una eventualidad.