BOLETÍN DTIC

9 de junio de 2022
Boletín 1
dtic@una.cr

Noticias, comentarios y anuncios tecnológicos

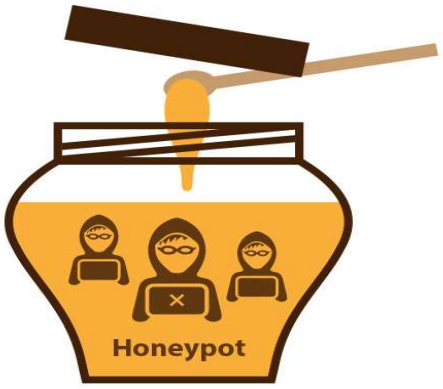
En esta edición:

Importancia de las contraseñas

Las contraseñas, claves o "passwords", han sido por décadas la forma de permitir y autenticar el ingreso de una persona a un sistema de información o solución tecnológica en general.

Como un conjunto de buenas prácticas, las contraseñas deben poseer letras mayúsculas y minúsculas, números y caracteres especiales. Debe evitarse que representen aspectos de nuestras vidas tales como nombres o fechas de cumpleaños. Siempre que se pueda, deben ser extensas, evitando el uso de contraseñas cortas o mínimas. En caso de ser posible, debemos incluir la recuperación de contraseñas extraviadas u olvidadas, mediante la configuración de un correo electrónico alterno y/o número de teléfono actualizado.

Evitemos compartir contraseñas que impliquen una responsabilidad o riesgo para los bienes que se encuentren a nuestro nombre, que permitan el acceso a información confidencial o personal a nuestro cargo, o a la custodia de datos de terceros, por ejemplo: sistemas de inclusión de calificaciones, aprobaciones en línea, sistemas bancarios (internet banking) y similares.



Cambios en las contraseñas

Por seguridad, las contraseñas deben ser cambiadas de forma periódica.

Según la circular UNA-CGT-CIRC-011-2022 / UNA-CGI-CIRC-003-2022 con fecha 16 de mayo de 2022, se comunican las siguientes acciones:

Clave unificada (funcionarios y estudiantes)

Se solicita cambiar esta contraseña de forma periódica a través del sitio http://www.claves.una.ac.cr

Correo electrónico institucional (funcionarios) y Office 365

El sistema solicitará el cambio obligatorio de contraseñas, cada 90 días.

¡Prepárese! Verifique con antelación los procedimientos asociados a la recuperación de contraseñas, en caso de extravío u olvido.

Honeypot

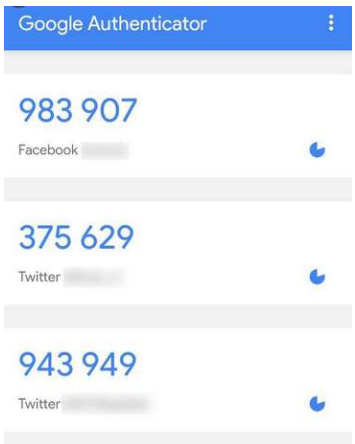
Un honeypot es un sistema tipo "señuelo" implementado para recibir ciberataques, permitiendo establecer patrones asociados al tipo de ataque informático recibido, cantidad y países de origen.

La idea es atraer a hackers – como la miel atrae a las abejas - para conocer los métodos utilizados en ciberataques.

Desde su implementación en agosto del 2021, este recurso ha recibido más de 1,5 millones de ataques, logrando determinarse que los nombres de usuario más utilizados para intentar infiltrarse en estos sistemas son admin, user, test, support; y las contraseñas más utilizadas son 123456, 12345, 1234, 123, password, admin, entre otras.

Los ataques recibidos particularmente han provenido de Vietnam, Estados Unidos, Alemania, Singapore, India, Países Bajos, Japón, Brasil, entre otros.

Este tipo de ataques, son recibidos de forma permanente de forma particular por los servidores web que se encuentran disponibles en la internet.



Segundo factor de autenticación

El segundo factor de autenticación (2FA) consiste en un mecanismo de seguridad adicional, equivalente a una "segunda contraseña", la cual es requerida para ingresar a un sistema de información o plataforma tecnológica.

Su utilización es conocida desde hace varios años mediante el uso obligatorio de "tokens" digitales o en plástico, que brindan las entidades bancarias como requisito obligatorio de ingreso a sus plataformas.

Se utilizan cada vez más en aplicaciones en general, como el correo electrónico.