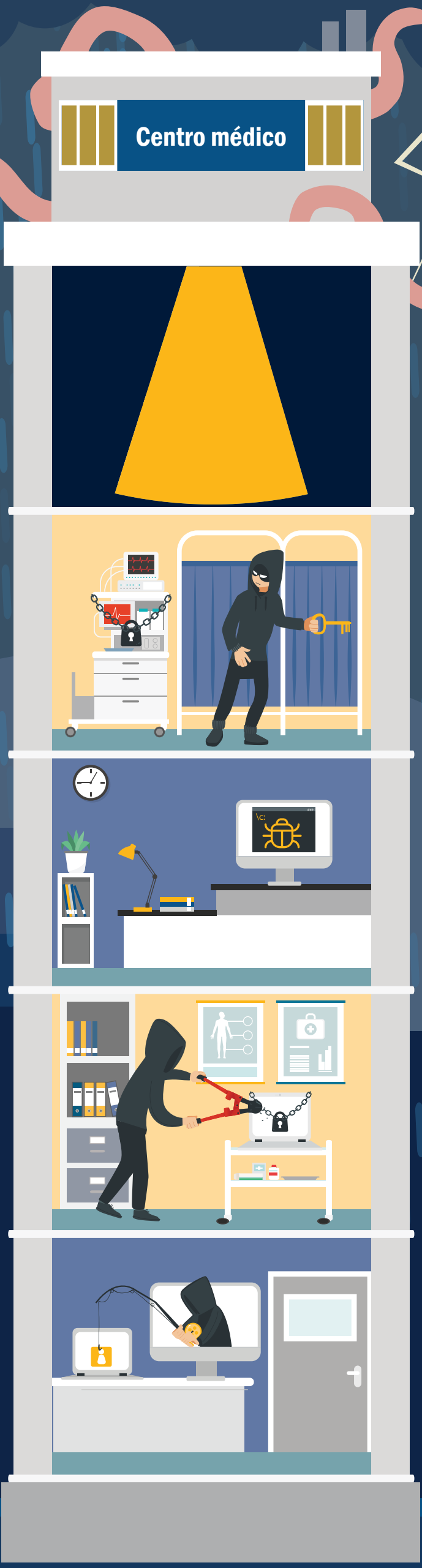
Escalamiento de amenazas en la atención médica

Existen muchas amenazas en algún nivel para todas las organizaciones de atención médica. Las amenazas pueden ser internas o externas, naturales o artificiales, maliciosas o accidentales. El impacto de estas amenazas en su organización depende de la capacidad de la amenaza para explotar las vulnerabilidades existentes. Es imperativo que sea consciente de las amenazas que pueden afectar a su entorno para proteger su valiosa información de salud protegida.



AMENAZA

Ataque de *ransomware*

El *ransomware* es un tipo de *malware* (software malicioso) cuya característica principal es que intenta denegar el acceso a los datos de un usuario, generalmente cifrando los datos con una clave que solo conoce el atacante que implementó el *malware*, hasta que se paga un rescate.

Ataque de denegación de servicio

Una vez que un virus infecta su red, un atacante puede implementar un ataque de denegación de servicio, lo que hace que los recursos de su red no estén disponibles en absoluto. Esto puede afectar la atención al paciente e interrumpir el servicio en toda su red, registros médicos y dispositivos médicos.

Ataque de virus

Una vez que se inyecta un virus en su entorno, puede ser perjudicial para su red al corromper el sistema o destruir datos de atención médica valiosos.

Ataque de fuerza bruta

Un atacante puede utilizar un ataque de fuerza bruta para obtener acceso a su red al intentar múltiples combinaciones de contraseñas numéricas hasta que se encuentre una coincidencia. Esto les permitirá acceder a su entorno donde se almacenan todos sus valiosos datos de información de salud protegida.

Ingeniería social

Muchos ataques comienzan con un correo electrónico de *phishing* que contiene un enlace malicioso y, si se hace clic en él, pueden crear graves riesgos de ciberseguridad para la red y la organización. El atacante podría obtener acceso a datos confidenciales de pacientes en manos de la organización.

Corrección

Audite sus aplicaciones de software en cada punto de conexión. Mantenga una lista de aplicaciones de software aprobadas. Elimine las aplicaciones de software no autorizadas tan pronto como se detecten.

Cree una referencia para su red y supervise la actividad inusual de la red. Si hay un gran pico en el tráfico, eso podría indicar un ataque volumétrico de denegación de servicio (DoS). Cualquier tipo de tráfico que se desvíe demasiado de la norma debe conducir a la cuarentena de un punto de conexión. Esto puede ayudar a mitigar el daño cuando se produce una infracción.

Las organizaciones deben asegurarse de que las soluciones básicas de software antispam/antivirus estén instaladas, activas y actualizadas automáticamente siempre que sea posible.

Limite la velocidad a la que pueden producirse los intentos de autenticación. Intente separar cada intento de contraseña uno o dos segundos, lo que puede limitar mucho la capacidad de los sistemas para forzar la contraseña con fuerza bruta.

La autenticación multifactor (Multi-Factor Authentication, MFA) debe implementarse en tecnologías de acceso remoto para limitar el valor de las credenciales de contraseña que podrían verse vulneradas mediante ataques de *phishing* o *malware*. La MFA es un método increíblemente efectivo para limitar la capacidad de un atacante de poner en peligro el entorno de su organización.

HHS 405(d)
Aligning Health Care Industry Security Approaches

Para obtener más información sobre cómo puede proteger a sus pacientes de las amenazas cibernéticas, consulte la publicación **Prácticas de ciberseguridad de la industria de la salud: gestión de amenazas y protección de pacientes**. Consulte los recursos disponibles que 405(d) tiene para ofrecer en nuestras páginas de redes sociales: **@ask405d** en **Facebook**, **Twitter**, **LinkedIn** e **Instagram**.