Fraude del CEO, phishing, ransomware – una protección más sólida frente a amenazas complejas: Retarus Advanced Threat Protection

El reto

Hoy en día, una gran parte del correo electrónico ya consiste en mensajes no solicitados. Además de la avalancha de correos electrónicos ordinarios de spam y virus, las empresas y los empleados están cada vez más expuestos a amenazas complejas como los ataques de ingeniería social y phishing. A menudo, los mecanismos de seguridad tradicionales ya no ofrecen suficiente protección contra estos correos electrónicos individualizados. Además, el malware también va mutando a intervalos cada vez más cortos y circula en variantes siempre nuevas.

La situación de partida

Cuando aparecen por primera vez, las nuevas amenazas son por su propia naturaleza desconocidas para los exploradores antivirus. Puesto que todavía no se dispone de las firmas adecuadas, el correo electrónico infectado se propaga en un periodo de tiempo muy corto. Además de esta situación, los ciberdelincuentes emplean métodos de ataque cada vez más sofisticados que los estafadores utilizan para acceder a información confidencial. Con las soluciones de seguridad tradicionales resulta complicado distinguir estos correos electrónicos de los mensajes legítimos. Los ataques perpetrados con éxito no solo provocan graves pérdidas de datos y fallos masivos del sistema, sino también enormes costes y daños a la reputación. Por tanto, las empresas necesitan urgentemente adaptar sus conceptos de seguridad informática a las circunstancias actuales.

La solución

El paquete **Essential Protection** de **Retarus Email Security** ya ofrece mecanismos de protección completos así como hasta cuatro exploradores antivirus diferentes que filtran de forma fiable la mayoría de los correos electrónicos peligrosos. Con la protección ampliada de **Advanced Threat Protection** (ATP), las empresas también pueden protegerse contra amenazas que van más allá de los virus clásicos y los mensajes de spam con numerosas funcionalidades adicionales.

Beneficios para el cliente

- Protección de comunicación comercial confidencial
- Seguridad informática con garantía de futuro
- Seguridad frente a pérdidas financieras por estafa
- Sensibilización de los empleados contra ataques de phishing y similares
- Protección contra daños de reputación por pérdida de datos

Resumen de ventajas

- Detección fiable de nuevas variantes de virus y malware
- Protección ampliada contra ataques de ingeniería social y otras amenazas complejas
- Análisis a través de fuentes de datos especializadas y algoritmos propios
- Informes y análisis detallados
- Integración perfecta de otros servicios de correo electrónico de la plataforma de Retarus

Caso de uso

Los atacantes utilizan cada vez más la ingeniería social para llevar a cabo ataques que conllevan el riesgo de daños financieros para las empresas. Por ejemplo, en el caso de estafas por fraude del CEO, los ciberdelincuentes se hacen pasar por el CEO de una empresa y piden a sus víctimas que transfieran grandes sumas de dinero en correos electrónicos falsos. **CEO Fraud Detection** de Retarus permite reconocer a tiempo las direcciones de remitente falsas utilizadas para estos ataques dirigidos y avisar a los empleados de correos electrónicos falsos. Además de un análisis avanzado del encabezado del correo electrónico, también se utilizan algoritmos especializados para identificar de forma fiable las denominadas suplantación de remitentes (From-Spoofing) y suplantación de dominios (Domain-Spoofing).

La característica **Retarus Time-of-Click Protection** también se puede utilizar para evitar ataques de phishing y la consiguiente pérdida de datos confidenciales. La tecnología comprueba todos los enlaces incluidos en los correos electrónicos para detectar direcciones de destino sospechosas de phishing. Primero, todos los enlaces en los correos electrónicos entrantes se reescriben automáticamente («URL Rewriting»). Cada vez que un destinatario hace clic en un enlace de este tipo, se comprueba de nuevo su potencial peligrosidad. Si mientras tanto se dispone de nueva información sobre la página de destino, esta se bloquea y en su lugar se muestra una advertencia de seguridad al usuario.

Para proteger mejor a las empresas de malware en constante evolución, como es el caso del ransomware, Advanced Threat Protection de Retarus incluye además la función **Deferred Delivery Scan** así como un análisis en profundidad mediante el método de **Sandboxing**. Deferred Delivery Scan consiste en una nueva exploración retrasada en el tiempo de los archivos adjuntos seleccionados. Para ello, la entrega del correo electrónico se retrasa unos minutos porque un nuevo análisis puede contener firmas de virus actualizadas después de un corto periodo de tiempo que no estaban disponibles en el momento del primer análisis. El Sandbox o análisis en entorno aislado, también incluido como parte de la solución Advanced Threat Protection, permite ejecutar primero los archivos adjuntos en un entorno de prueba virtual y seguro antes de su entrega, donde se comprueba su comportamiento inusual mediante procedimientos de simulación complejos.

¿Sabía que...?

Cada día se registran más de 390.000 programas maliciosos nuevos en todo el mundo. Esto se traduce en una media de alrededor de 270 nuevas variantes de virus por minuto.

Otros escenarios

Postdelivery Protection

La innovadora tecnología **Patient Zero Detection®** de Retarus identifica los correos electrónicos peligrosos que ya han sido enviados. En caso de sospecha, se informa inmediatamente a los destinatarios y administradores para evitar daños mayores.

Cifrado seguro

Los datos confidenciales nunca deben caer en las manos equivocadas. Gracias a **Retarus Email Encryption** (compatible con PGP, OpenPGP y S/MIME), las empresas pueden proteger la confidencialidad de sus comunicaciones e implementar fácilmente las leyes de protección de datos aplicables.

Email Live Search

Como parte de Retarus Essential Protection, **Email Live Search** ofrece un análisis rápido de la entrega del correo electrónico. Gracias a ello, el equipo de asistencia puede realizar un seguimiento detallado de qué mensajes que pasaron por la infraestructura, en qué momento y qué filtros de seguridad se aplicaron.