TEMPEST/TERA

LOS NIVELES DE SEGURIDAD GUBERNAMENTALES MEJORADOS CON EL SISTEMA DE CABLEADO TERA®

Los problemas de seguridad de TI son un tema controversial. Si bien es cierto que la seguridad siempre ha estado presente en la mente del gerente de TI, la reciente avalancha de Información, regulación y productos relacionados con la seguridad de la red son bastante nuevas en el sector privado. Sin embargo, eso no ocurre en el caso de las redes gubernamentales y militares, las cuales han puesto la seguridad dentro de sus prioridades y este enfoque han dado como resultado parámetros y procesos de seguridad extremadamente sólidos.

En el sector privado, la seguridad de la información generalmente se basa en medidas tales como firewalls, contraseñas, datos biométricos y tarjetas de acceso. Por otro lado la información gubernamental en sus distintos niveles, puede incluir datos del departamento de defensa, de salud y servicios humanos y/o información de infraestructura. Los niveles de seguridad están dictados por la naturaleza de los datos, y en redes gubernamentales clasificadas como seguras, la capa física del cableado está incluida en las medidas de seguridad.

La seguridad del sistema de información se puede dividir en categorías como: Personal, la parte Física y Operativa, de Información y Electromagnética. El Personal representa el nivel más vulnerable, ya que pagar a los trabajadores por acceso o información es el método de explotación menos costoso, menos riesgoso y más rápido. La falta de protección física permite que un adversario obtenga acceso a la instalación, al sistema, al cableado y a la información directamente, pero con un riesgo moderado. Una buena seguridad operacional minimizará los errores en la configuración y operación de los sistemas y limitará las formas en que la información confidencial puede filtrarse. La seguridad de la información evitará el acceso externo a la misma mediante cifrado, cortafuegos y otras medidas de protección de flujo de bits. La seguridad electromagnética sirve para evitar la recepción de emanaciones de señales de equipos y cables que permitirían a un adversario a cierta distancia interceptar y decodificar señales de las comunicaciones.

TEMPEST/TERA

Las medidas de seguridad del cableado se dividen en múltiples categorías. La seguridad física debe implementarse para evitar el acceso no controlado externo al cableado y al equipo. El gobierno utiliza los Sistemas de Distribución Protegida (PDS) (conducto pegado, tubería, alarmas, monitoreo de video, etc.) para proteger físicamente el cableado que atraviesa áreas no controladas.

Se necesitan medidas operativas para documentar y etiquetar la infraestructura de cableado y equipos para minimizar la posibilidad de permitir por error transmitir información confidencial/clasificada en medios no controlados o permitir el acceso de personal no confiable al cableado y equipos sensibles. El etiquetado de distribución permitirá la inspección y el control de acceso para detectar conexiones de cable no autorizadas. Todos los puntos de terminación del cable deben estar etiquetados y controlados, y es importante comprender que se debe hacer para cada punto de entrada y salida en una red. La documentación y la inspección periódica sirven para abordar los posibles puntos de incumplimiento de la red y los incumplimientos reales. La documentación de la capa física se puede lograr mediante paneles inteligentes, modificaciones automáticas a dibujos o bases de datos, entrada de nuevas etiquetas en puntos de terminación o una combinación de estos. Dichos pasos son fácilmente empleados por el sector privado y cada vez se incorporan más a la gestión de redes en empresas no gubernamentales.

Más allá de limitar la accesibilidad física, las señales emitidas de la planta de cableado deben limitarse. El control de todas las emanaciones comprometidas dentro de los espacios controlados es fundamental para las comunicaciones gubernamentales que requieren un alto nivel de seguridad tales como la Seguridad Nacional. El gobierno lo denomina EMSEC (Seguridad de Emisiones), INFOSEC (Seguridad de la Información) y TEMPEST. Estos programas/clasificaciones funcionan para asegurar que las señales normalmente emitidas estén protegidas de algún modo de públicos sin escrúpulos que usarían esta información capturada para medios no autorizados.

Las señales emitidas o las emisiones se producen en todos los equipos informáticos y en todos los cables de cobre. En los Estados Unidos, la FCC controla la cantidad de emisiones permitidas y existen homólogos internacionales para este propósito (documentos IEC CISPR). La variedad no deseada de emisiones de señal se conoce como emanaciones comprometedoras. Las emanaciones comprometedoras pueden transmitirse a través de líneas eléctricas, cableado de datos y teléfono, o simplemente irradiarse por el aire. Cuando se recibe o se intercepta una emisión comprometedora, la información segura puede verse comprometida cuando las señales se pueden reconstituir en la información confidencial original. Los microchips, los transistores de diodos y otros componentes electrónicos no lineales en los equipos de procesamiento de datos son una fuente potencial de emanaciones comprometedoras. Las señales en los cables de cobre, especialmente las señales de datos donde las transiciones bruscas producen señales de alta frecuencia significativas pueden crear emanaciones comprometedoras.

TEMPEST es un Código de gobierno de los Estados Unidos que define los estándares de contrainteligencia desarrollados para proteger las transmisiones de datos seguras contra el espionaje electrónico. Aunque los requisitos reales están clasificados, es ampliamente conocido que TEMPEST establece límites estrictos sobre la emisión de la señal de los equipos electrónicos de manejo de datos. Si bien el alcance de la información TEMPEST publicada se centra en equipos físicos como monitores, impresoras y dispositivos que contienen microchips, el término se usa comúnmente para describir los esfuerzos en todo el campo de la Seguridad de Emisiones (EMSEC). EMSEC se define como "la protección resultante de todas las medidas diseñadas para negar a las personas no autorizadas la información que pueda derivarse de la intercepción y el análisis de emanaciones comprometedoras de otros equipos criptográficos y sistemas de telecomunicaciones", según el Comité ANSI/TIA.

TEMPEST/TERA

TEMPEST comenzó hace muchos años cuando se determinó que las transmisiones se podían detectar al aire libre desde una distancia significativa al escuchar las emisiones de un cable. En 1918, el ejército de los EE. UU. Contrató a Herbert Yardley y su personal de la Cámara Negra para desarrollar métodos para detectar, interceptar y explotar teléfonos de combate y transmisores de radio encubiertos. Sin embargo, la palabra clave TEMPEST no se usó hasta los años 60 y 70. Hay varias definiciones para el acrónimo que incluyen "Material electrónico de telecomunicaciones protegido contra transmisiones espurias emanantes" y Estándar de emanación de pulso electromagnético transitorio". Sin embargo, estos acrónimos son algo especulativos, ya que el título oficial, junto con sus requisitos, están clasificados. En resumen, TEMPEST es el medio para proteger transmisiones y cubre medios, dispositivos de comunicación y otras medidas de protección.

Aunque la transmisión, recepción y prueba de emisiones de señales se denomina TEMPEST, los criterios de implementación diseñados para minimizar esto se denominan ROJO / NEGRO. ROJO comúnmente se refiere a información sensible de texto claro, y NEGRO serían las señales cifradas o no clasificadas. Los requisitos y criterios básicos ROJO / NEGRO se desclasificaron en 1995 como NSTISSAM TEMPEST / 2-95 (FOUO). Los límites de emisión reales y los parámetros de prueba permanecen clasificados. Incluso sin parámetros más completos, se sabe que TEMPEST sirvió como modelo para los programas equivalentes de muchos otros gobiernos. El equivalente de la OTAN es AMSG 720B. En Alemania, incluso los nombres de los estándares suministrados por el gobierno permanecen clasificados, pero se sabe que la Junta Nacional de Telecomunicaciones administra su equivalente al programa de calificación TEMPEST. En el Reino Unido, la Sede de Comunicaciones del Gobierno (GCHO), el equivalente de la NSA (Administración de Seguridad Nacional), administra su programa.

Si bien, en Estados Unidos solo existe un estándar TEMPEST, existen tres niveles de aprobación de nivel de cifrado de la NSA en Estados Unidos. El tipo 1 es aceptable para su uso en equipos criptográficos clasificados o controlados y puede referirse a ensamblajes, componentes u otros elementos avalados por la NSA para proteger las telecomunicaciones y los sistemas automatizados para la protección de información clasificada o sensible del gobierno de Estados Unidos. Este equipo está sujeto a restricciones de acuerdo con las Regulaciones Internacionales de Tráfico de Armas. La aprobación de tipo 2 es para equipos, conjuntos y componentes utilizados en la transmisión de información confidencial pero no clasificada. Tipo 3 implementa un algoritmo no clasificado registrado en el Instituto Nacional de Estándares y Tecnología (NIST) para su uso en la protección de información confidencial o comercial no clasificada.

La certificación TEMPEST de Estados Unidos puede aplicarse tanto a equipos como a sistemas completos en un entorno de red. Existen procedimientos separados de prueba TEMPEST para equipos en un laboratorio y para sistemas en el campo. Las pruebas TEMPEST de campo y de laboratorio incluyen todos los componentes del sistema con pruebas de campo que incluyen la planta de cableado como parte de la prueba TEMPEST. Cambiar un solo componente puede comprometer la seguridad de todo el sistema. En comunicaciones seguras, el medio utilizado para transmitir los datos (es decir, el cableado) es parte del sistema TEMPEST o EMSEC. Los estándares de control de emisiones TEMPEST para equipos y cableado, combinados con encriptación de datos y otros sistemas de seguridad, permiten INFOSEC (Seguridad de la Información). Debido a estos estrictos requisitos, el gobierno históricamente ha tenido pocas opciones para la seguridad de la capa física (cableado).

Una opción efectiva de cableado TEMPEST es el uso de redes de fibra óptica. Esto proporciona protección adicional debido a que la fibra no irradia / emite señales y tendría que estar físicamente comprometida para poder acceder a las comunicaciones. Sin embargo, el equipo de red de fibra es más costoso que los componentes de cobre equivalentes, lo que resulta en mayores costos de mantenimiento ya que se basan en el precio de compra original y requieren más mantenimiento que el cobre.

TEMPEST/TERA

Las redes de cobre se usan comúnmente, pero requieren prácticas de instalación muy específicas, como las pautas de separación NSTISSAM TEMPEST / 2-95 RED / BLACK. En ROJO / NEGRO, el cableado y el equipo ROJO están separados y / o protegidos del cableado y el equipo NEGRO para evitar el acoplamiento. El equipo y el cableado RED están restringidos al acceso externo, así como a la proximidad a otros radiadores de señal potenciales. Otros equipos que pueden escuchar, transportar o propagar emisiones, como teléfonos celulares y radios, están prohibidos en las áreas ROJAS.

La mayoría de las agencias federales que se ocupan de información clasificada han capacitado a las Autoridades Técnicas Certificadas TEMPEST (CTTA) para asesorar y aprobar instalaciones de sistemas clasificados. Los CTTA tienen una formación y antecedentes TEMPEST significativos para permitirles equilibrar los criterios de seguridad ROJO / NEGRO con la amenaza para el sistema para proporcionar una solución de seguridad TEMPEST óptima de costo beneficio. Hay menos necesidad de seguridad TEMPEST en ciertas situaciones, como aquellas en las que hay un gran espacio controlado o inspeccionable alrededor del sistema seguro, y más necesidad de seguridad TEMPEST donde el espacio controlado o inspeccionable es mínimo. Solo una Autoridad Técnica Certificada TEMPEST puede determinar el espacio inspeccionable y los criterios de protección IAW NSTISSI 7000.

El cable de cobre blindado proporciona una capa adicional de seguridad al limitar significativamente las emisiones. Si bien esto en teoría permitiría reducir las distancias de separación ROJO / NEGRO, las prácticas de instalación TEMPEST pueden no permitir esta reducción en la práctica. Se requiere cable blindado según el nivel de seguridad, el espacio inspeccionable y la amenaza. El uso de cable blindado puede reducir las separaciones de cable, eliminar o reducir la necesidad de aislamiento y filtrado de la señal, generalmente se requiere para su uso con equipos aprobados por TEMPEST y reducir o eliminar la necesidad de cable adicional u otro blindaje. El cable blindado también se puede utilizar para la señalización NEGRA para reducir las posibilidades de que estos cables capten otras señales emanadas.

El F / UTP o cable blindado tiene un blindaje de aluminio general que rodea cuatro pares trenzados sin blindaje y se usa tradicionalmente cuando se especifica un cable blindado, aunque esto puede no ser suficiente en algunas situaciones. Se puede proporcionar un aislamiento de señal adicional a través de escudos trenzados, pares más apretadas, blindaje de pares individuales con un escudo de aluminio general. Los sistemas de distribución metálicos y la instalación en sí también pueden proporcionar aislamiento de señal. Se debe seleccionar un cable y una configuración que limiten las señales emanadas dentro del espacio controlado o inspeccionable.

Las pruebas recientes arrojan información adicional sobre los estándares y las opciones de cobre para las conexiones a TEMPEST y otros equipos de procesamiento seguro. El sistema TERA® de Siemon, un sistema de cobre de Categoría 7 / Clase F, pasó la prueba de emisiones TEMPEST por un laboratorio independiente certificado por la NSA, Dayton T. Brown Inc. en una configuración específica. Esto indica que el cableado TERA debe cumplir con todos los requisitos de cableado blindado TEMPEST incluso en las situaciones más exigentes. Aunque el cableado en general no puede ser aprobado por TEMPEST, ya que las señales y la configuración variarán, la configuración de cableado blindado TERA proporcionará la mejor protección TEMPEST disponible.

Si bien la mayoría de los parámetros de prueba son información clasificada, se entiende que la combinación de conectividad TERA y cable minimiza / elimina las emisiones como parte de un sistema general. TERA utiliza cable S/FTP y conectividad totalmente blindada. En el cable S/FTP, cada par está blindado individualmente y un blindaje de trenza general rodea todos los conductores. El blindaje adicional está integrado en las salidas y enchufes, eliminando otra fuente potencial de emisión. Es importante tener en cuenta que un sistema 6A F/UTP no pasó la misma prueba cuando se usó un solo cable blindado con láminas con conectores RJ45.

TEMPEST/TERA

Para la prueba TEMPEST, se desplegó un canal TERA de cuatro conectores y 100 metros en una cámara anecoica blindada. El canal se energizó con tráfico Gigabit Ethernet dúplex completo (1000 Mb/s) utilizando un sistema de análisis multipuerto Spirent Smarbits. Las emisiones del sistema de cableado fueron monitoreadas y comparadas con los requisitos TEMPEST, con las emisiones del cable TERA sin exceder los requisitos TEMPEST. Las emisiones de los sistemas de cable TERA no excedieron los requisitos de emisión de TEMPEST y superaron la misma configuración utilizando un solo cable blindado de lámina con RJ 45 (que tenía emisiones que excedían los límites permitidos).

Según el informe de la prueba independiente, el cable TERA es adecuado para aplicaciones como TEMPEST donde las emisiones emitidas y comprometedoras son una preocupación. El resto del informe de prueba es información clasificada. El cable TERA debe usarse con equipos TEMPEST, ya que proporciona mayor seguridad de limitar las emanaciones de cable a las del equipo TEMPEST. El cable TERA también se puede usar para otros tipos de señales (análogas, datos síncronos, video, otra red de velocidad, etc.), y en lugar de conductos adicionales, edificios u otro blindaje, donde TEMPEST de alta calidad y otra reducción o eliminación de emisiones sea necesario.