

El antivirus, una necesidad corporativa

Ricardo Villadiego, gerente de ventas para Colombia y Ecuador de Trend Micro, habló en exclusiva para Channel Planet. El tema central de la entrevista fue la seguridad en los sistemas y las soluciones como los antivirus.

El antivirus, una necesidad corporativa Ricardo Villadiego, gerente de ventas para Colombia y Ecuador de Trend Micro, habló en exclusiva para Channel Planet. El tema central de la entrevista fue la seguridad en los sistemas y las soluciones como los antivirus. Bogotá, Colombia, 6 de junio de 2003. Redacción Channel Planet. Natalia Camacho. redaccion@channelplanet.com natalia@channelplanet.com Channel Planet acostumbra a diseñar contenidos exclusivos para nuestros clientes; estos tienen relación con el contenido de los eventos. Teniendo en cuenta que uno de nuestros próximos seminarios será IT Security 2003 (16 y 17 de julio), hemos entrevistado a algunos ejecutivos de las empresas más importantes de la industria tecnológica. Les presentamos, la primera de ellas. Channel Planet: En su opinión, ¿Cuál cree que es la percepción del mercado corporativo frente a soluciones como los antivirus? Ricardo Villadiego: En términos generales existe la conciencia de que son necesarias las soluciones de antivirus. Sin embargo, hace unos años el concepto de antivirus se popularizó tanto que cayó en el común denominador, de forma que cada compañía sabía que debía tener un antivirus sin importar cual.

Paralelamente a esto el desarrollo de código malicioso creció a tal punto de convertirse en lo que hoy se llaman ataques de amenaza mixta, que aprovechan el concepto de replicación que tiene un virus con otro tipo de amenazas como caballos de troya o troyanos, gusanos, backdoor etc. Con lo cual hoy para una compañía es muy importante determinar cual es la herramienta ideal de antivirus, el esquema de protección que ofrece y la forma como realmente le agrega valor a la compañía. C.P: Realmente el mercado es consciente de la necesidad de tener un antivirus en sus organizaciones? R.V: Si es consciente porque es un común denominador, es como salir a carretera y saber que es obligatorio llevar el equipo de carreteras, el problema es que muchos (y me incluyo) nunca sabemos si el extinguidor realmente va a funcionar. La diferencia con el símil anterior es que hoy el mayor número de incidentes de seguridad que viven las compañías están asociados al tema de virus y código malicioso en general con lo cual la seriedad con la cual el tema debe ser abordado debe ser mucho mayor, las empresas deben estar seguras que están eligiendo la plataforma antivirus y anti código malicioso que realmente soluciona sus problemas en los tiempos y con la proactividad con las que se necesita responde al tema de ataques de amenaza mixta. C.P: En materia de seguridad, considera usted que Colombia tiene esta cultura, y cómo es este aspecto frente a otros países de América Latina? R.V: Afortunadamente es una cultura creciente, con certeza se puede decir hoy que la cultura de seguridad informática del 2003 es significativamente mayor a la del 2000.

La pregunta tal vez debe ser si tenemos la cultura adecuada de seguridad informática, aquí mi percepción muy particular es que todavía estamos reaccionando por "moda" o por "reacción pura – un ataque-". El tema de virus es uno de los muchos escenarios que vale la pena mencionar, si el 85% o más de los incidentes de seguridad de una compañía están asociados a código malicioso y virus en general, la seriedad con la que se debería atacar el tema debe ser mucho mayor. C.P: Podría darnos unas recomendaciones generales acerca de la inversión en el área de seguridad que una compañía debe tener en cuenta a la hora de tomar una decisión? R.V: Es aventurado recomendar en este aspecto. Lo mejor que una compañía puede hacer es crear un modelo de seguridad y determinar cuanto valen sus riesgos. Pues de llegar a materializarse esto, automáticamente generara un presupuesto de seguridad y las acciones que se pueden tomar. Es como si usted tiene un carro que vale 20 millones de pesos,

claramente no tienen ningún sentido comprarle una alarma que cueste los mismos 20 millones, o comprarle un seguro que cueste los mismos 20 millones. Así mismo, en el caso de virus por ejemplo si la cuantificación del riesgo de una epidemia en la empresa arroja aproximadamente 30 mil dólares y en un año se pueden esperar 4 posibles epidemias (este año ya llevamos una alerta roja y dos amarillas) probablemente no tenga mucho sentido gastarse mas de US\$ 120K en protección antivirus para esta empresa, pero con certeza tiene todo el sentido del mundo implementar la solución adecuada antivirus que impida perder 120 mil dólares en epidemias en el primer año. Pero en general los presupuestos en seguridad deben mostrar sentido de negocio y la mejor forma de mostrar sentido de negocio es atándolos al riesgo potencial que experimenta una compañía. C.P: ¿Cuáles serían las aplicaciones que una empresa debe adquirir para tener unos sistemas seguros? R.V: Igual todo depende del análisis de riesgo, sin embargo la teoría de seguridad de la información se fundamenta en una estructura basada en tres pilares: (Integridad, Confidencialidad y Disponibilidad) después hay miles de tecnologías: de autenticación, de encriptación, de control de acceso, de detección de intrusos, de clustering, de antivirus, de antispam, entre otros. Todos finalmente tienden a proteger alguno de los tres pilares básicos. Igualmente, los ataques de seguridad tienden en su forma más básica a violar alguno de estos tres pilares básicos de seguridad. Existen ataques como los de amenaza mixta de código malicioso que tienen la propiedad de poder atacar al tiempo los tres pilares básicos de la seguridad de la información: LOVEGATE, que fue una de las recientes alertas amarillas podía afectar la disponibilidad del canal de Internet, alterar la integridad de los archivos en servidores, estaciones, etc y violar la confidencialidad de la información instalando un backdoor (puerta trasera) en las estaciones para permitirle a un intruso tomar acceso no autorizado a la estación de trabajo. En fin saquen sus propias conclusiones. C.P ¿Qué ofrece Trend Micro en antivirus y soluciones de seguridad informática? R.V: Trend Micro esta 100 por ciento enfocada en el segmento de código malicioso y seguridad de contenido, en este orden de ideas, tenemos soluciones antivirus para todos los puntos de entradas a una red, empezando desde la estación de trabajo, pasando por el servidor de correo electrónicos, servidores de archivos, gateway de internet (smtp, pop3, imap, http) y computadoras de mano (palms). En el lado de contenido tenemos soluciones antispam con tecnologías basadas en listas negras en heurística, filtros de correo electrónico para garantizar el uso adecuado del correo electrónico en una corporación y evitar las molestas cadenas y la pérdida de información crítica de la empresa vía correo electrónico; y soluciones de URL Screening para garantizar el uso adecuado de la navegación en Internet de los empleados de una empresa.

Eliana Salgado, 06 de junio de 2003

Enlace original:

<http://www.channelplanet.com/?idcategoria=10885>

