DELL EMC

Seguridad para el trabajador moderno

Faculte a los empleados para que trabajen a su manera y, a la vez, proteja los datos en todas partes.

En la actualidad, los datos están en constante movimiento, lo que supone nuevas amenazas para la seguridad. La TI debe poder abordar estos riesgos nuevos sin restringir el flujo de información. Esta es la conclusión de un informe reciente de Forrester, *Evolving Security to Accommodate the Modern Worker.** Brett Hansen, vicepresidente de software cliente y gerente general de seguridad de los datos, comparte información valiosa acerca del informe y de las soluciones que ofrece Dell para satisfacer las necesidades de los empleados y de la TI.

¿Por qué es importante proteger los datos?

Esta pregunta tiene tres respuestas. La primera es que existen normativas que exigen proteger ciertos tipos de datos. En la mayoría de los casos, se trata de los datos de clientes, como la información de los pacientes en los servicios de salud o la información de los empleados. El incumplimiento de estos requisitos conlleva consecuencias cada vez más graves. Entonces, la protección de los datos es un requisito mínimo.

En segundo lugar, hoy en día los datos son vitales para las empresas. Independientemente del sector en el que se encuadre, los datos son la parte más importante del negocio y, si están en riesgo, los resultados pueden ser catastróficos para el estado de una empresa. La tercera es la reputación de la marca. La capacidad de proteger los datos de la empresa es una expectativa que se comparte universalmente. Tanto si se trata de cumplir con leyes de protección de datos como de reconocer la importancia de los datos como la base del negocio o de proteger la reputación de la marca, estos tres aspectos son fundamentales.

El informe de Forrester señala que los empleados consideran que la seguridad los hace menos productivos. ¿Por qué cree que sucede esto?

Las empresas emplean soluciones de seguridad y establecen políticas que son cada vez más restrictivas.

> “Independientemente del sector en el que se encuadre, los datos son la parte más importante del negocio y, si están en riesgo, los resultados pueden ser catastróficos para el estado de una empresa”.
>
> **Brett Hansen,**
> Vicepresidente de software cliente y gerente general de seguridad de los datos en Dell

Es mucho más seguro tomar los datos y guardarlos bajo llave en un ambiente hermético en el que nadie pueda acceder a ellos, pero el propósito de tener datos es poder usarlos. Los empleados desean obtener información valiosa de la base de datos de los clientes, colaborar con colegas y compartir las mejores prácticas. Todas estas acciones requieren la transferencia de datos.

Los profesionales de TI no intentan poner más dificultades a los empleados para que realicen su trabajo. Simplemente, utilizan soluciones más

tradicionales basadas en elementos heredados. Si observamos las políticas y las tecnologías implementadas el año pasado, estas obstaculizan lo que las personas desean hacer con los datos, que es colaborar y aumentar el impulso del negocio.

¿Cómo podemos encontrar un punto intermedio entre la TI y los empleados? ¿Puede la TI adaptar las soluciones de seguridad a los distintos trabajadores y las distintas ocupaciones?

Esto comienza con una conversación. Los profesionales del negocio y el equipo de seguridad cibernética deben sentarse y hacerse las preguntas "¿cuál es la estrategia de nuestra línea de negocios?" y "¿qué intentamos hacer desde la perspectiva de las personas?".

Lo siguiente es saber que no hay una única solución para todo. Las organizaciones y los grupos que las componen tienen distintos requisitos. Las políticas y la tecnología deben reflejar distintas necesidades. Lo que sucede habitualmente es que la TI impone una política de seguridad común a todos, en lugar de considerar quiénes son estas personas, cuáles son sus objetivos y qué herramientas necesitan para proteger los datos confidenciales.

¿Cuán flexible puede ser la seguridad para abordar las necesidades de los distintos tipos de trabajadores?

Es una combinación de políticas y herramientas. Deben implementarse las políticas correctas, que surgen de una estrategia de seguridad más amplia que informa a los empleados lo que pueden y no pueden hacer. Los empleados desean recibir capacitación. Quieren tener estas conversaciones y desean que se los faculte. Sin embargo, las empresas necesitan herramientas que las protejan, debido a que se enfrentarán a amenazas externas y posibilidades de riesgos. En relación con la flexibilidad, la respuesta es simplemente "sí, se puede hacer", lo que nos lleva nuevamente a "todo comienza con una conversación".

Usted mencionó que los empleados desean sentirse facultados. El informe de Forrester señala que los trabajadores están dispuestos a administrar su propia seguridad. ¿Cree que están preparados para manejar esto?

La respuesta simple a esa pregunta es no. Una de las conclusiones del informe de Forrester fue que el 62 %

de los empleados señalan que les preocupa el hecho de que se los culpe de una vulneración de seguridad.* Eso es muy sorprendente. Todo el mundo vive con una preocupación constante. Debería haber una sensación de confianza de que los empleados conocen las medidas que deben adoptar para proteger los recursos de la empresa y, a continuación, se debería incluir un conjunto de funcionalidades que les permitiera hacerlo. Los empleados son personas y las personas cometen errores y tienen accidentes, pero lo que se puede hacer es alinear las capacitaciones de manera tal que los empleados se sientan facultados. Deben comprender los tipos de políticas de seguridad que se implementan, de modo que puedan adoptarlas, en lugar de oponerse a ellas. Este enfoque, combinado con prácticas de seguridad que les den la libertad de trabajar a su manera, reforzará la seguridad y la confianza.

¿Cuál es el enfoque de Dell respecto de la protección de datos? ¿Qué soluciones logran mejor este objetivo y en qué nos diferenciamos de la competencia?

Hay algunas características que hacen que Dell sea único. Estamos hace menos tiempo que muchas otras empresas en el área de la seguridad. Eso es bueno. Dado que no tenemos un portafolio heredado que aborde problemas de seguridad obsoletos, estamos mucho mejor posicionados para impulsar soluciones que se adecuen a la fuerza de trabajo y los retos actuales.

Abordamos la amenaza de los atacantes externos con Dell Endpoint Security Suite Enterprise (con tecnología de Cylance), un enfoque sin firmas de aprendizaje automático para detectar malware y detener las amenazas externas. Ponemos la mirada en el propio código subyacente, lo que hace que sea mucho más

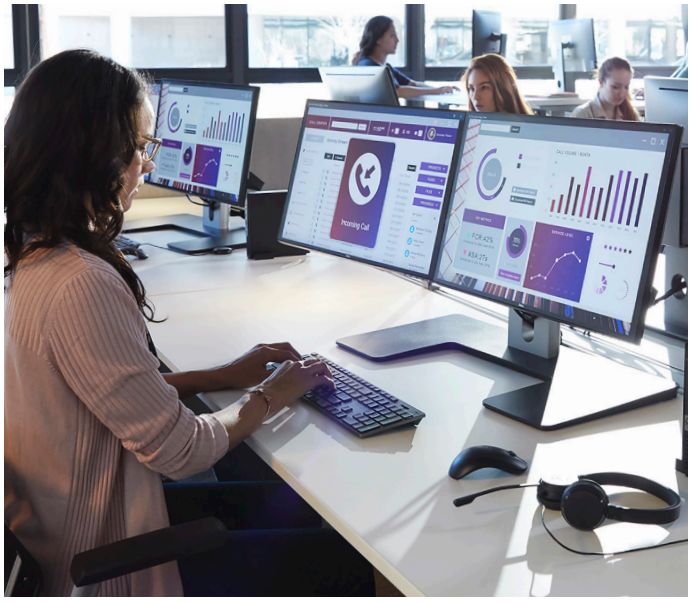
difícil que los atacantes oculten sus intenciones. Y el aprendizaje automático causa un impacto mínimo en el sistema, ya que la máquina escanea los archivos en busca de malware potencial, incluso cuando se escanean cientos de puntos de datos. Las soluciones heredadas que buscan firmas frenarán por completo un sistema.

Por último, protegemos a las personas de ellas mismas. Si las políticas impiden que los empleados realicen su trabajo, estos encontrarán una manera de eludirlas. No son intencionalmente maliciosos. Solo intentan realizar su trabajo de la manera más eficiente posible. En lugar de levantar muros y guardar los datos bajo llave, nuestras herramientas, como Dell Data Guardian, permiten que los empleados realicen su trabajo y que la TI proteja, controle y monitoree los archivos sin importar dónde se encuentren. Nuestro proceso ofrece varias facetas de defensa: detenemos a los malhechores y, a continuación, protegemos a los usuarios internos de ellos mismos.

> “Si se crea un ambiente en el que los empleados pueden trabajar de manera eficiente, y además se cuenta con un nivel de confianza y funcionalidades para proteger los datos, el aumento de la productividad se producirá naturalmente”.
>
> **Brett Hansen,**
> Vicepresidente de software cliente
> y gerente general de seguridad de los datos en Dell

¿Cómo la protección y el aseguramiento de los datos fomenta la productividad?

Si se crea un ambiente en el que los empleados pueden trabajar de manera eficiente, y además se



cuenta con un nivel de confianza y funcionalidades para proteger los datos, el aumento de la productividad se producirá naturalmente. Volvemos al tema de la reunión entre el negocio y la seguridad cibernética. Deben tener una conversación y establecer una estrategia en conjunto.

En una situación ideal, el negocio y la TI están alineados y cuentan con una estrategia, pero en el momento de la verdad, la seguridad debe avanzar con las políticas. Independientemente de la posición del negocio y la seguridad, Dell puede proporcionar herramientas que permiten que la TI y los empleados dispongan de lo mejor de ambos mundos. Los empleados pueden mantener la productividad sin temor a crear una vulneración. Si volvemos a revisar la estadística que indica que al 62 % de los empleados les preocupa crear una vulneración*, no estamos en presencia de un ambiente óptimo. Queremos que los empleados se sientan seguros de saber lo que están haciendo. Facultémoslos de una manera que permita controlar los riesgos. La tecnología está disponible. Solo es necesario que las empresas reconozcan este nuevo paradigma y adopten estas herramientas.

* Según un estudio realizado por Forrester Consulting y encargado por Dell, *“Evolving Security to Accommodate the Modern Worker”*, octubre de 2017.