Consejos de ciberseguridad: La Propiedad Intelectual de tu empresa está en riesgo

Actualmente, la **propiedad intelectual** (PI) no se limita en absoluto a unos pocos secretos comerciales estrechamente guardados, como recetas y patentes de propiedad. Ahora, la Propiedad Intelectual adopta una amplia variedad de formas, desde planes estratégicos hasta investigaciones competitivas, diseños patentados y código informático.

En segundo lugar, la propiedad intelectual, como la mayoría de la información, ahora se almacena principalmente en formato digital. Además, no hay un solo almacén digital: los datos críticos se distribuyen en varias bases de datos, repositorios de código, plataformas de colaboración, sistemas de mensajería e incluso en la memoria de dispositivos como impresoras y copiadoras. Lo que es peor, tu equipo de TI podría incluso administrar necesariamente todos los sistemas que alojan tu PI pero las aplicaciones modernas son tan fáciles de implementar que el "Shadow IT" T se ha convertido en algo común.

2021 pondrá un riesgo de propiedad intelectual a la vanguardia

En 2021, con la recesión económica mundial y las incertidumbres empresariales causadas por la pandemia, la protección de la propiedad intelectual será más vital que nunca. De hecho, evitar una fuga de PI podría fácilmente significar la diferencia entre la supervivencia y el colapso de un negocio.

En este 2021, una amenaza será especialmente urgente: el riesgo de propiedad intelectual que plantean los usuarios en el entorno de TI. Hay varias realidades empresariales detrás de esta predicción. A medida que las organizaciones buscan mantenerse dinámicas, contratarán a personas por proyecto y proveedores a corto plazo. Eso significa que habrá más usuarios en el entorno de TI pero menor lealtad corporativa y menos capacitación para ayudarles a reconocer ataques como **phishing y prácticas peligrosas** como copiar datos confidenciales en laptops o insertar dispositivos USB en dispositivos conectados a la red.

Al mismo tiempo, los equipos de TI siguen luchando para facilitar la productividad de los equipos remotos. Cuando la pandemia llegó, tuvieron que implementar rápidamente nuevas aplicaciones en la nube y migrar usuarios y datos, y ahora están bastante ocupados tratando de corregir la seguridad y otras brechas que quedaron a raíz de esos esfuerzos apresurados. Como resultado, hay más posibilidades de que los equipos de TI cometan errores o tomen vías rápidas.

Por último, muchos de los empleados a tiempo completo siguen trabajando desde casa, donde los límites pueden parecer más borrosos. Se comunican y colaboran a través de plataformas y aplicaciones, como **SharePoint Online y Microsoft Teams**, en lugar de cara a cara donde las pistas visuales como diferentes colores a menudo dificultan saber quién es una persona externa a la organización y quién no.

Por lo tanto, es posible que no estén prestando tanta atención como deberían a quién tiene acceso a los datos que están compartiendo. De hecho, la tendencia en las aplicaciones modernas ha sido descentralizar el control, por lo que los usuarios empresariales son capaces de crear fácilmente sus propios sitios y equipos. Es posible que no tengan la formación para centrarse en la seguridad de la propiedad intelectual cuando se centren en hacer su trabajo, por lo que es posible que no piensen dos veces en incluir a los trabajadores temporales en sus chats, listas de distribución, equipos, etc.

Reducción del riesgo de propiedad intelectual en 2021

También existen buenas noticias: la clave para reducir el riesgo de fuga de propiedad intelectual es seguir estas prácticas recomendadas de TI.

En particular, debes:

- La **aplicación de privilegios** mínimos incluye no solo garantizar un aprovisionamiento preciso, tener una visión profunda de los permisos eficaces y controlar el uso compartido externo en Office 365.
- Presta mucha **atención a Microsoft Teams**: Teams es una potente plataforma de colaboración, lo que lo convierte en un vector importante para la fuga de PI. En particular, asegúrate de comprender cómo se pueden agregar usuarios invitados a los equipos y qué pueden hacer una vez que están dentro.
- Controlar el **uso compartido de datos en SharePoint**: SharePoint también es un canal eficaz para la transferencia de información. Los archivos almacenados en un sitio de SharePoint suelen estar disponibles para todos los usuarios con permisos para el sitio, y los usuarios pueden compartir archivos específicos, o incluso un sitio completo, con otros también. Presta especial atención a la configuración que controla el uso compartido externo y el uso de enlaces anónimos o “cualquiera”.
- Realiza una **auditoría minuciosa** de los cambios y otras actividades: independientemente de la precaución con la que configures el entorno, aún tendrás que vigilar de cerca lo que sucede día a día. Debes estar atento a la actividad que podría poner en peligro la seguridad de la PI, incluidos los cambios en los objetos de Active Directory el comportamiento inusual de los usuarios. Idealmente, debes obtener alertas en tiempo real, ser capaz de llevar a cabo investigaciones rápidas y exhaustivas, y la capacidad de bloquear objetos críticos.
- **Simplifica y automatiza las tareas de TI**: Saca a los equipos de TI del modo de lucha contra incendios para que puedan ser proactivos en la protección de la PI. Hacer que los procesos críticos pero rutinarios, como la copia de seguridad y recuperación, la generación de informes y la administración de Active Directory, sean lo más sencillos e infalibles posible mediante la automatización.