'Bossware': un recorrido por las aplicaciones de vigilancia en el teletrabajo

BENNET CYPHERS, KAREN GULLO :: 08/09/2020

Los jefes pueden retroceder a través del día de un trabajador y ver lo que estaban haciendo en un momento determinado

El COVID-19 ha obligado a millones de personas a trabajar desde casa, y una multitud de marcas de software para vigilancia de trabajadores se han lanzado a promocionar masivamente sus productos a las empresas de todo el mundo.

A menudo el software al que nos referimos es presentado como relativamente inocuo: Algunos proveedores lo comercializan como software para "el seguimiento automático de tiempo" o de "análisis del lugar de trabajo", mientras que otros productos se dirigen a empresas preocupadas por el robo de propiedad intelectual o el robo de datos. Nosotros llamamos a estas herramientas, conjuntamente, *bossware*.

Si bien la pretensión comercial de estos productos es ayudar a las empresas, queremos explicar por qué el *bossware* pone en peligro la privacidad y la seguridad laboral de los trabajadores. Por ejemplo, en algunos casos, estos programas están diseñados para registrar cada clic y cada interacción con el teclado y para recopilar información de forma encubierta con fines punitivos o disciplinarios, además de utilizar otras funciones de espionaje que van mucho más allá de lo que es necesario y proporcionado para organizar el teletrabajo.

Aunque el hogar se convierta en una oficina, sigue siendo un hogar. Los trabajadores no deben estar sujetos a vigilancia no consensuada ni a ser controlados en sus propios hogares para mantener sus empleos.

¿Qué pueden hacer estas herramientas?

El *bossware* normalmente se aloja en un ordenador o en un smartphone y tiene permiso para acceder a los datos de ese dispositivo. La mayoría del *bossware* recoge aproximadamente todo lo que hace el usuario. Hemos revisado publicidad, demos y comentarios de los clientes para hacernos una idea completa de cómo funcionan estos programas. No obstante, dada la gran cantidad de programas de este tipo que se encuentran actualmente en el mercado, vamos a desglosar las diferentes formas de vigilancia que existen por categorías.

El tipo más amplio y común de vigilancia es el “monitoreo de actividades". Normalmente, el monitoreo abarca también un registro de las aplicaciones y sitios web que visitan los trabajadores, por ejemplo, las herramientas de mensajería (el *bossware* revisará desde el asunto del email hasta otras clases de metadatos) y cualquier publicación que se realice en redes sociales. La mayoría de los programas también registran los niveles de entrada del teclado y del ratón y muchos de ellos ofrecen un desglose de cuánto teclea y hace clic

minuto a minuto un usuario, bajo la premisa de llevar a cabo un registro de la productividad. El software de vigilancia tratará de reunir todos estos datos en sencillos gráficos que ofrezcan a los empleadores un resumen detallado de la diligencia de los trabajadores.

Todos los productos que hemos revisado realizan continuas capturas de pantalla de los dispositivos. En algunos casos, llegan a emitir vídeo en directo. Después, esta enorme cantidad de contenido audiovisual es organizada en una línea de tiempo, de modo que los jefes pueden retroceder a través del día de un trabajador y ver lo que estaban haciendo en un momento determinado.

Varios productos actúan como registros de teclas, anotando cada pulsación, incluyendo correos electrónicos no enviados y contraseñas privadas. Dos de ellos permiten incluso a los administradores entrar y tomar el control del escritorio de un usuario. Es importante señalar, que este proceso de registro no suele distinguir entre la actividad laboral y las credenciales de las cuentas personales, los datos bancarios o la información médica.

Algunos tipos de *bossware* van más allá, llegando al mundo físico que rodea a los dispositivos. Las empresas que ofrecen software para dispositivos móviles casi siempre incluyen el seguimiento de la ubicación utilizando el GPS. Al menos dos servicios -StaffCop Enterprise y CleverControl- permiten a los empleadores activar secretamente las cámaras y los micrófonos del ordenador o del teléfono móvil.

En general, el *bossware* puede ser instalado de dos formas: como una aplicación visible para el trabajador (y tal vez incluso manipulable por él) o como un proceso silencioso que los trabajadores no pueden ver. La mayoría de las empresas que hemos estudiado dan a los empleadores la opción de instalar su software de ambas maneras, que recogemos como vigilancia visible e invisible.

Vigilancia visible

Hay situaciones en que los trabajadores pueden reconocer el software que los vigila y tienen la opción de activar o desactivar la vigilancia, como una forma de fichar las entradas y salidas del horario laboral. Por supuesto, el hecho de que un trabajador haya desactivado la vigilancia será visible para su empleador. Por ejemplo, con Time Doctor, los trabajadores tienen la opción de eliminar determinadas capturas de pantalla de su sesión de trabajo; sin embargo, al borrar una captura de pantalla también se borrará el tiempo de trabajo asociado, de modo que los trabajadores sólo serán remunerados por el tiempo durante el cual se les supervisa.

Los empleados pueden tener acceso a una parte o a toda la información que se recopile sobre ellos. Crossover, la empresa que está detrás de WorkSmart, compara su producto de vigilancia con una aplicación de entrenamiento deportivo. Su interfaz permite a los trabajadores ver los resultados del sistema sobre su actividad presentados en una serie de gráficos y tablas.

El nivel de transparencia hacia los trabajadores dependerá de la marca. Algunas dan a los trabajadores acceso a una cantidad variable de información. Otras, como Teramind, indican

simplemente que están encendidas y recabando datos, pero no revelan todo lo que están recogiendo. En cualquiera de los casos, a menudo el usuario no tiene claro qué información se está seleccionando exactamente, a no ser que lo consulte directamente con su superior o se examine cuidadosamente el propio programa informático.

Vigilancia invisible

La mayoría de las compañías que construyen software de vigilancia visible también crean productos que tratan de esconderse de las personas que están monitoreando. Teramind, Time Doctor, StaffCop, y otras compañías hacen productos que están diseñados para ser tan difíciles de detectar y eliminar como sea posible. A nivel técnico, estos productos son indistinguibles de un troyano. De hecho, algunas marcas para ser instaladas requieren que los empleadores reconfiguren específicamente el antivirus antes de instalar sus productos, para que este no detecte y bloquee la actividad no deseada.

Aunque este software se comercializa con un propósito específico (la supervisión de trabajadores), la mayoría de estos productos también sirven como herramientas de vigilancia de carácter general. StaffCop ofrece una versión de su producto específicamente diseñada para supervisar el uso de Internet por parte de los niños, y ActivTrak afirma que su software también puede ser utilizado con este mismo fin por padres o profesores. Los comentarios de los clientes sobre algunos de los programas indican que muchos de ellos los utilizan en sus hogares.

La mayoría de las empresas que ofrecen vigilancia invisible recomiendan que sólo se utilice para los dispositivos en propiedad de la compañía. Sin embargo, muchas también ofrecen características como la instalación remota y “silenciosa” del software en los dispositivos privados de los trabajadores, incluso si estos están fuera del lugar de trabajo. Esto es posible porque muchos empleadores tienen privilegios de acceso en los ordenadores que distribuyen. El problema radica en que para algunos trabajadores el portátil de la compañía es su único dispositivo, por lo que la supervisión de la empresa está siempre presente, facilitando un posible uso excesivo por parte de los empleadores. Es posible que las víctimas nunca sepan que están sujetas a tal vigilancia.

¿Es habitual el *bossware*?

El negocio de la vigilancia de los trabajadores no es nuevo y ya era bastante importante antes de la pandemia mundial. Si bien es difícil evaluar cuán común es el *bossware*, sin duda se ha vuelto mucho más habitual a medida que los trabajadores se ven obligados a trabajar desde sus hogares debido al COVID-19. Awareness Technologies, propietaria de InterGuard, afirmó haber aumentado su base de clientes en más de un 300% en sólo las primeras semanas después del estallido de la pandemia y muchos de los vendedores que hemos estudiado explotan el auge del COVID-19 en sus campañas de marketing.

Algunas de las empresas más grandes del mundo usan bossware. Los clientes de Hubstaff incluyen a Instacart, Groupon y Ring. Time Doctor afirma tener 83.000 usuarios; sus clientes incluyen a Allstate, Ericsson, Verizon, y Re/Max. ActivTrak es utilizado por más de 6.500 organizaciones, incluyendo la Universidad Estatal de Arizona, la Universidad de Emory y las ciudades de Denver y Malibú. Compañías como StaffCop y Teramind no revelan

información sobre sus clientes, pero afirman ser empleados por sectores como el cuidado de la salud, la banca, la moda, la industria manufacturera y los *call centers*. Las valoraciones que hacen los propios clientes de estas marcas nos pueden dar más ejemplos de cuánto se ha extendido el uso de estos programas.

No sabemos cuántas de estas organizaciones optan por utilizar la vigilancia invisible, ya que los propios empleadores no suelen publicitarlo. Además, no hay una forma fiable de que los propios trabajadores lo sepan, ya que muchos programas informáticos invisibles están diseñados explícitamente para eludir la detección. Algunos trabajadores tienen contratos que autorizan ciertos tipos de vigilancia e impiden otros, pero para muchos de ellos puede ser imposible saber si están siendo vigilados. Por esta razón, aquellos que se preocupen por esta posibilidad deben asumir que cualquier dispositivo proporcionado por el empleador los está vigilando.

¿Para qué se utilizan los datos?

Las marcas de *bossware* comercializan sus productos para una amplia variedad de usos. Algunos de los más comunes son el seguimiento del tiempo y de la productividad, el cumplimiento de las leyes de protección de datos y la prevención del robo de propiedad industrial o intelectual. En algunos casos, su uso puede resultar razonable: por ejemplo, las empresas que tratan con datos confidenciales están obligadas asegurarse de que estos no sean filtrados o se roben de sus sistemas. Si los empleados trabajan fuera de la empresa, puede requerir un cierto nivel de supervisión en el dispositivo. Sin embargo, un empleador no debería realizar ningún tipo de vigilancia con fines de seguridad a menos que pueda demostrar que es necesaria, proporcionada y adecuada para los problemas que está tratando de resolver.

Lamentablemente, en muchos casos los empleadores ejercen un poder no justificado sobre sus trabajadores. La mayoría de los productos que hemos examinado están diseñados para la "supervisión de la productividad" o para un mejor seguimiento del tiempo de trabajo; es decir, para registrar todo lo que hacen los trabajadores y asegurarse de que están trabajando lo suficientemente duro. Algunas empresas consideran que sus herramientas son una ventaja potencial tanto para los empresarios como para los trabajadores. Recopilar información sobre cada segundo del día de un trabajador no sólo es bueno para las compañías, afirman, sino que supuestamente también ayuda al trabajador. Otros proveedores, como Work Examiner y StaffCop, se dirigen explícitamente a los gerentes que no confían en su personal. Estas empresas suelen recomendar que se vinculen los despidos o las bonificaciones a las evaluaciones de rendimiento derivadas de sus productos.

Algunas empresas comercializan sus productos directamente como instrumentos punitivos o como herramientas para recopilar indicios contra los trabajadores. InterGuard anuncia que su software "puede ser instalado silenciosamente y de forma remota, para que usted pueda llevar a cabo investigaciones encubiertas [de sus trabajadores] y reunir datos *a prueba de balas* sin alarmar al sospechoso". Esta prueba, continúa, puede ser usada para luchar contra "reclamaciones frente al despido". En otras palabras, InterGuard puede proporcionar a los empleadores una cantidad astronómica de información privada y secreta para tratar de anular los recursos legales de los trabajadores contra el trato injusto.

Ninguno de estos casos de uso, ni siquiera los menos perturbadores mencionados anteriormente, justifican la cantidad de información que el *bossware* recopila. Y nada en absoluto excusa que se oculte el hecho de que la vigilancia se está llevando a cabo.

La mayoría de los productos hacen periódicamente capturas de pantalla, y solo algunos de los programas permiten a los trabajadores elegir cuáles compartir. Esto implica que la información médica, bancaria o personal sensible se captura junto a emails trabajo y redes sociales. Los productos que incluyen registradores de teclas son aún más invasivos y a menudo terminan capturando las contraseñas de las cuentas personales de los trabajadores.

Descripción de Work Examiner de su función de registro de teclas, destacando específicamente su capacidad para capturar contraseñas privadas.

Desafortunadamente, la excesiva recopilación de información a menudo no es un accidente, sino una prestación más. Work Examiner anuncia específicamente la capacidad de su producto para almacenar contraseñas privadas. Otra empresa, Teramind, informa sobre cada dato que se introduce en un correo electrónico a un cliente, incluso si esa información se borra posteriormente. Varios programas también analizan cadenas de texto de mensajes privados en redes sociales para que los empleadores puedan conocer los detalles más íntimos de las conversaciones de los trabajadores.

Seamos claros: este software está diseñado específicamente para ayudar a los empleadores a leer los mensajes privados de los trabajadores sin su conocimiento ni su consentimiento. En cualquier caso, esto es innecesario y poco ético.

¿Qué se puede hacer?

Amparados por la legislación de los Estados Unidos, los empleadores tienen demasiada libertad para instalar software de vigilancia en los dispositivos que poseen. Además, poco les impide coaccionar a los trabajadores para que instalen este software en sus propios dispositivos (siempre y cuando la vigilancia se pueda desactivar fuera del horario laboral). Los estados tienen diferentes normas sobre lo que los empleadores pueden y no pueden hacer. En cualquier caso, es habitual que los trabajadores tengan pocos recursos legales frente al software de vigilancia intrusiva.

Eso puede y debe cambiar. A medida que las legislaciones de los estados y del país continúan adoptando leyes de privacidad de los datos de los consumidores, también deberían establecer sistemas de amparo para los trabajadores con respecto a sus empleadores. Para empezar:

La vigilancia de los trabajadores, incluso en los dispositivos en propiedad del empleador, debe ser imprescindible y proporcionada. Los dispositivos deben reducir al mínimo la información que recogen y evitar la captura de datos personales como mensajes privados y contraseñas. Los trabajadores deben tener derecho a saber qué información están recopilando sus empleadores. Y los trabajadores necesitan recursos legales para que puedan demandar a los empleadores que violen estas protecciones legales de la privacidad.

Mientras tanto, los trabajadores que estén en conocimiento de la vigilancia ejercida por la

empresa podrán establecer un diálogo con la misma para alcanzar pactos y las empresas que han incorporado el *bossware* deberán considerar cuáles son sus objetivos y tratar de alcanzarlos de la manera menos intrusiva. De hecho, el *bossware* a menudo incentiva los tipos de productividad inadecuados, por ejemplo, forzando a la gente a pasear deliberadamente el ratón y a escribir cada pocos minutos en lugar de leer o detenerse a pensar. El monitoreo constante puede ahogar la creatividad, disminuir la confianza y contribuir al agotamiento. En el caso de que a los empleadores les preocupe la seguridad de los datos protegidos, deberían considerar herramientas que se adapten específicamente a las amenazas reales y que reduzcan al mínimo los datos personales atrapados en el proceso.

Si el trabajador sospecha que su empleador le está vigilando y desconoce el alcance de la situación, debería asumir que los dispositivos de trabajo capturan y recopilan todo, desde el historial web hasta los mensajes privados y las contraseñas. Si es posible, deberá evitar el uso de los dispositivos de trabajo para fines personales. Y si se pide a los trabajadores que instalen software de vigilancia en sus dispositivos personales, deberían solicitar a sus empleadores un dispositivo alternativo específico para el trabajo.

Por último, es posible que los trabajadores no se sientan cómodos cuestionando la vigilancia por la preocupación de perder el trabajo en un momento de desempleo récord. La elección entre la vigilancia y el desempleo no debería ser una elección en absoluto.

El COVID-19 ha creado nuevas tensiones en todos nosotros, y es probable que también cambie fundamentalmente la forma en que trabajamos. Sin embargo, no debemos dejar que marque el comienzo de una nueva era de vigilancia. Vivimos más que nunca a través de nuestros dispositivos, haciendo fundamental el derecho de mantener nuestras vidas digitales en privado, alejadas de gobiernos, empresas tecnológicas y de nuestros empleadores.

eff.org. Traducción: Guillem Matas Cerdán para Sinpermiso. Extractado por La Haine.

---

https://www.lahaine.org/mundo.php/bossware-un-recorrido-por-las