Definición de los temas de actualidad sobre seguridad en Internet, diferencias entre países

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Index

1. Introducción

Hoy en día, casi toda la información está *online* y casi todos los actos de una persona común tienen algún impacto: huella en la RED (redes sociales, correos electrónicos, transferencias de dinero, *cookies*, etc.).

Además, en estos días casi todo tiene conexión directa en la RED y gracias a la 4ta revolución industrial, esto es solo un comienzo.

El objetivo principal de este informe es resumir las conclusiones más importantes con respecto a dos temas: ciberseguridad y seguridad web y datos personales y seguridad en Internet.

Además, como vimos en el informe anterior, existen muchas similitudes en los países involucrados en este proyecto con respecto a los temas mencionados anteriormente. Por lo tanto, las diferencias existentes entre países están más relacionadas con algunas cláusulas iniciales que dejan margen de maniobra a los legisladores nacionales.

2. Conclusiones principales

En esta sección tenemos una lista de las principales conclusiones que fueron localizadas en los Resultados Intelectuales 2- Aspectos legales de la seguridad en Internet. Las conclusiones se dividen en dos temas.

2.1. Ciberseguridad y seguridad en la red

2.1.1 Trabajo / Empresas

- Los ataques son cada vez más complejos y frecuentes y la principal motivación detrás de los ataques es la monetización;
- La seguridad en la nube se está convirtiendo en un problema crítico y se espera que las empresas dependan cada vez más de los proveedores de la nube;
- La importancia de las medidas organizativas (por ejemplo, gestión de riesgos) aumentará en el futuro en comparación con las medidas puramente técnicas;
- La dependencia de las empresas de productos de *hardware* y *software* representa una amenaza creciente;
- No hay suficientes incentivos para las inversiones en seguridad en las empresas;
- Falta de conciencia y estándares de seguridad;
- La falta u obsolescencia de fundamentos legales en los países que dificultan la comprensión y la aplicación de medidas de seguridad;
- Falta de conciencia acerca de seguridad por parte de la mayoría de los empleados;
- Falta de personal capacitado / cualificado en seguridad cibernética y competencias digitales;
- Falta de actividades de capacitación para mejorar el conocimiento y un comportamiento mucho más seguro por parte de las personas;
- Falta de conocimiento de los empleados sobre las amenazas cibernéticas y las reglas de seguridad de TI;
- Falta de guías técnicas claras y concisas relacionadas con la ciberseguridad y la seguridad en Internet;
- El aumento de los requisitos salariales del personal cualificado en ciberseguridad puede complicar la situación;

- Muchas herramientas de seguridad separadas aumentan en última instancia la complejidad operativa y reducen la visibilidad de la postura general de seguridad;
- Las organizaciones a menudo no tienen un equipo formal de respuesta a incidentes de seguridad cibernética o incluso una persona nombrada responsable de lidiar con dicho incidente;
- Existe una falta de colaboración entre los equipos de privacidad y seguridad cibernética;
- Muchas compañías no tienen un plan de respuesta de ciberseguridad consistente;
- Falta de tiempo y recursos cualificados necesarios para implementar el plan de seguridad cibernética;
- Falta de un presupuesto adecuado necesario para aumentar las capacidades de seguridad;
- Hardware y software de seguridad de TI obsoletos;
- Falta de compromiso por parte de la administración junto con un presupuesto insuficiente;
- Falta de participación entre todos los trabajadores en la estrategia de ciberseguridad (si existe);
- El inventario de activos con impacto en ciberseguridad no es bien conocido por todos los trabajadores de la empresa;
- La cultura de ciberseguridad necesita ser interiorizada, programas y medidas de seguridad como procesos, gestión ambiental o de prevención de riesgos laborales;
- Pocas iniciativas centradas en la ciberseguridad industrial;
- No hay soluciones de ciberseguridad suficientemente probadas;
- Falta de cooperación entre la empresa y las iniciativas gubernamentales;
- Comunicación ineficiente entre los diferentes equipos debido a sus diferencias con respecto a sus conocimientos y capacidades sobre el uso de software y hardware;
- Hay actividades que pueden poner en peligro los sistemas y, como consecuencia, la seguridad de los procesos e instalaciones industriales;
- Falta de conocimiento de los efectos y de la necesidad de nuevas tecnologías utilizadas para asegurar la interoperabilidad de los sistemas de control;
- Percepción general de que la amenaza es incierta y bastante improbable;
- El espionaje por medios digitales modernos amenaza la competitividad y la productividad nacional;

- Diferentes necesidades de ciberseguridad entre diferentes sectores de actividad;
- Falta de apoyo financiero para el desarrollo de la seguridad cibernética;
- Escasez o falta absoluta de estándares específicos para la seguridad cibernética;
- Malentendidos del tema debido a la escasez de programas de capacitación enfocados y material de comunicación pública;
- Implementación incorrecta de soluciones y tecnologías de seguridad como firewalls, soluciones IDS / IPS, antivirus, etc.
- Ninguna relación o acuerdo entre autoridades, empresas y proveedores en relación con la ciberseguridad;
- Escasez de coordinación entre los diferentes estados miembros de la UE.

2.1.2. Vida privada

- Falta de conciencia y estándares de seguridad;
- Comportamientos negligentes al usar internet;
- Los programas actuales de las escuelas de pregrado no incluyen, la mayoría de las veces, temas de seguridad cibernética;
- Aunque existen buenas iniciativas, consejos y sugerencias, pero no llega a la población en general;
- Gran cantidad de software malicioso en el mercado;
- Comprensión inadecuada del estado del ciberataque;
- Hay muchas áreas rurales en las que no hay muchas ofertas de capacitación adicionales debido a la ubicación;
- La ayuda suele darse con dificultades y generalmente solo está disponible por teléfono o en línea (a excepción de acudir directamente a la policía). Se necesita un punto de contacto, con el cual las personas también puedan contactar directamente en caso de experimentar problemas;
- Los reglamentos, políticas y leyes no están formulados de manera fácil para el usuario;
- La información sobre los materiales de apoyo a veces es muy difícil de encontrar (en Internet) y necesita un acceso más rápido y sencillo;
- Usar una contraseña débil, una contraseña para iniciar sesión en varias cuentas y no cambiar la contraseña;

- Falta de materiales de estudio sobre ciberseguridad;
- Las personas confían fácilmente en los archivos adjuntos de correo electrónico;
- Las personas comparten mucha información personal en las redes sociales;
- Falta general de interés de los jóvenes sobre la seguridad en Internet;
- Falta de conocimiento de las amenazas cibernéticas y las reglas de seguridad de TI;
- No hay muchas plataformas de ciberseguridad para intercambiar y compartir información;
- Falta de apoyo financiero para la promoción de la seguridad de Internet para las personas y el desarrollo de la ciberseguridad;
- Pocas iniciativas centradas en la seguridad de Internet en la vida cotidiana;
- Escasez de programas educativos y de capacitación y materiales públicos sobre seguridad en Internet;
- Baja alfabetización digital de los usuarios finales;
- Falta conocimiento básico de amenazas potenciales de los usuarios públicos;
- No se ha creado una cultura de seguridad cibernética;
- Falta de guías técnicas claras y concisas sobre seguridad en Internet y seguridad cibernética;
- El inventario de activos con impacto en ciberseguridad no se conoce bien;
- Falta de conocimiento de los efectos y la necesidad de nuevas tecnologías utilizadas para asegurar la interoperabilidad de los sistemas de seguridad / control;
- Mala comprensión de la seguridad cibernética y de Internet debido a la escasez de programas de capacitación enfocados a este área y material de comunicación pública;
- Las políticas y procedimientos no son adecuados desde el punto de vista de la ciberseguridad;
- Los riesgos de ciberseguridad no están integrados en herramientas y sistemas;
- No hay soluciones de ciberseguridad suficientemente probadas;
- Implementación incorrecta de soluciones y tecnologías de seguridad como firewalls, soluciones IDS / IPS, antivirus, etc.
- Poca coordinación entre los diferentes estados miembros de la UE.

2.2. Protección de datos personales y seguridad en Internet

- Las nuevas normas relativas a la protección de datos personales impondrán considerables demandas a las empresas;
- Todavía faltan, existen fundamentos legales obsoletos e información simple en países que dificultan la comprensión y la aplicación de Reglamento General de Protección de Datos (GDPR) y otra legislación de protección de datos personales;
- La existencia de divergencias con respecto a la información, las medidas y los procedimientos necesarios para una implementación adecuada del GDPR ya que muchas empresas aún no saben exactamente qué hacer;
- La necesidad de tener acceso a información simple y clara e información fácil de usar;
- Falta / baja implementación de medidas para aumentar la protección de datos personales a diario;
- Falta de medidas, consejos y capacitación accesible con respecto a la protección de datos personales para todos, independientemente de su edad, conocimiento o ubicación geográfica;
- Falta de actividades de capacitación desde las primeras etapas;
- Desarrollar la ciudadanía digital del estudiante a través de la tecnología apropiada, incluida la etiqueta de comunicación en línea y los derechos y responsabilidades digitales;
- Los europeos piden una mayor protección de la privacidad en línea;
- Muchas empresas aún reconocen la necesidad de reforzar la información y la capacitación de los trabajadores con respecto al GDPR;
- La mayoría de las empresas necesitan una primera evaluación relacionada con el nivel de conformidad y la adecuación de las políticas y procesos actuales para una identificación correcta de posibles cambios con respecto al GDPR;
- Los desafíos reales relacionados con la modernización, la globalización, la tecnología y la digitalización implican una revisión del proceso GDPR que ya existe de manera continua;
- Involucrar a toda la comunidad implicada en la protección de datos personales lo antes posible;

- Definir y revisar, con frecuencia, los conocimientos, habilidades, atributos y otras características para las que las personas pueden y deben ser capacitadas, con respecto a los temas en análisis;
- Estimular la producción de contenido creativo y educativo en línea para todas las personas que debe ser simple y accesible para todos;
- Las tecnologías digitales cambian constantemente y los maestros / formadores necesitan recibir capacitación constante para poder ayudar y brindar actividades de capacitación apropiadas;
- Designar responsabilidades de protección de datos para su equipo;
- Mantener una documentación detallada de los datos que está recopilando, cómo se usan, dónde se almacenan, qué empleado es responsable de ellos, etc.
- Capacitar a su personal e implementar medidas de seguridad técnicas y organizativas.

2.3. Ciberseguridad en Europa

Durante los últimos años, la Comisión Europea ha introducido una serie de medidas como alternativa para garantizar un entorno en línea más seguro en la UE. Además, la Comisión Europea está trabajando para aumentar las capacidades y la cooperación en ciberseguridad, fortalecer a la UE como un actor de ciberseguridad en todo el mundo.
Desde 2017, la UE comenzó a comprometerse más a proporcionar medidas de ciberseguridad y a aumentar la confianza de los ciudadanos y las empresas en la sociedad digital en Europa, pero fue hasta junio de 2019 (con el Reglamento (UE) 2019/881 del Parlamento Europeo) que implementaron una serie de medidas destinadas a desarrollar una fuerte ciberseguridad dentro de la UE y la seguridad del entorno digital de la UE. Además, la Ley de Ciberseguridad es parte de la ciberseguridad general de la UE y establece algunos requisitos de notificación y seguridad para los operadores de servicios esenciales y proveedores de servicios digitales como los proveedores de la nube.

Además, desde junio de 2019, la Ley Europea de Ciberseguridad entró en vigor estableciendo el nuevo mandato de ENISA, la Agencia de Seguridad Cibernética de la UE y estableciendo el marco de certificación europeo de ciberseguridad.

Aun cuando hay una legislación sobre seguridad cibernética que está en vigor en cada estado miembro, también hay algunas cláusulas de apertura que dejan a los legisladores nacionales un margen de maniobra con respecto a la implementación de la seguridad cibernética. Algunos de los países de Europa (República Checa, Austria, Portugal y España) tienen algunas legislaciones/directivas/códigos que abordan cuestiones de ciberseguridad en sus propios países. Sin embargo, las regulaciones de seguridad cibernética aún necesitan un mayor desarrollo, pues el Parlamento Europeo actúa como colegislador y cada estado miembro es el principal responsable de su propia seguridad cibernética. Por lo tanto, es necesario implementar algunas medidas para mejorar la resistencia cibernética, tales como:

- La legislación sobre seguridad cibernética sigue siendo incompleta y hay algunas demoras relacionadas con este tema en todo el territorio europeo. Como resultado, es necesario mejorar el intercambio de información y la coordinación entre los actores de la legislación y los sectores público y privado deben colaborar para contribuir a responder a los problemas de seguridad cibernética que puedan surgir;
- Los responsables políticos y los legisladores deben desarrollar una legislación más simple y directa que sea fácil de usar para todos, sin importar los antecedentes de la persona;
- Según un informe realizado por el Tribunal de Cuentas Europeo "Desafíos para una política efectiva de ciberseguridad de la UE", el 80% de las empresas de la UE experimentaron al menos un incidente de ciberseguridad en 2016; El 69% no tiene, o solo tiene una comprensión básica de su exposición a las amenazas cibernéticas y el 60% nunca ha estimado las posibles pérdidas financieras. Debido a esto, la seguridad cibernética en las empresas debe ser una de las principales prioridades y debe evaluarse periódicamente a través de algunas auditorías / análisis externos (por ejemplo, cada año). Con estas auditorías, las organizaciones tienen acceso a información útil y saben en qué necesitan centrarse / desarrollar. Debido a ello, tienen la responsabilidad de implementar algunas acciones para tener un mejor rendimiento de seguridad cibernética;
- La legislación por sí sola no garantiza la resiliencia y para construir una cultura de resiliencia cibernética, cada empresa debe tener un plan proactivo y también

reactivo para responder a algunos incidentes de seguridad cibernética que puedan ocurrir;

- También es imperativo tener una visión general clara de las necesidades de capacitación y debilidad de cada persona con respecto a esta área. Por lo tanto, aumentar las habilidades y la conciencia de las personas desde las primeras etapas es obligatorio y debe comenzar lo antes posible en cada país. Por ejemplo, es importante organizar algunas iniciativas y comenzar a implementarlas en empresas, escuelas y en el hogar. De acuerdo con esta sugerencia, por ejemplo, las empresas deben tener una persona certificada / cualificada en el área de ciberseguridad que pueda brindar capacitación al resto de los equipos, especialmente en el área de software y los incidentes cibernéticos más comunes, tales como: ataques de phishing; malware; Troyanos; correo no deseado; ransomware y datos robados. Esto también es importante para desarrollar una cultura de ciberseguridad.

Todas las sugerencias mencionadas anteriormente buscan lograr un mayor nivel de ciberseguridad en la UE y también tienen una respuesta más efectiva a los incidentes cibernéticos.

3. Catálogo de contenido sistematizado

A continuación se describen los apartados más importantes con respecto a los dos temas analizados en el Resultado Intelectual 2.

- **Seguridad en la nube:** también conocida como seguridad informática en la nube, consiste en un conjunto de políticas, controles, procedimientos y tecnologías que trabajan en conjunto para proteger los sistemas, los datos y la infraestructura basados en la nube. Estas medidas de seguridad están configuradas para proteger datos, respaldar el cumplimiento normativo y proteger la privacidad del cliente, así como establecer reglas de autenticación para usuarios y dispositivos individuales;
- **Cibercrimen:** cualquier actividad delictiva que involucre un ordenador, un dispositivo en red o una red. Si bien la mayoría de los delitos informáticos se llevan a cabo para generar ganancias para los delincuentes cibernéticos, algunos delitos informáticos se llevan a cabo contra ordenadores o dispositivos directamente para dañarlos o desactivarlos, mientras que otros usan ordenadores o redes para difundir *malware*, información ilegal, imágenes u otros materiales. El delito cibernético puede incluir muchos tipos diferentes de actividades delictivas con fines de lucro, incluidos ataques de *ransomware*, correo electrónico, fraude en Internet y fraude de identidad, así como intentos de robo de información de cuenta financiera, tarjeta de crédito u otra tarjeta de pago;
- **Ciberseguridad:** la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ataques cibernéticos generalmente tienen como objetivo acceder, cambiar o destruir información confidencial, extorsionar a los usuarios o interrumpir los procesos comerciales normales;
- **Robo cibernético:** robo de información financiera y / o personal a través del uso de ordenadores para su uso fraudulento u otro uso ilegal;
- **Violaciones de datos:** una divulgación intencional o no intencional de información segura o privada / confidencial a un entorno no confiable. Las violaciones de datos pueden involucrar información de salud personal, información de identificación personal, secretos comerciales y / o propiedad intelectual;
- **Fugas de datos:** transmisión no autorizada de datos (electrónica o físicamente) de una organización a un destino externo. Las amenazas de fuga de datos

generalmente ocurren a través de la web y el correo electrónico, pero también pueden ocurrir a través de dispositivos de almacenamiento de datos móviles como USB, *pen drives*, ordenadores portátiles, etc.

- **Protección de datos:** proceso de protección de datos e implica la relación entre la recopilación y difusión de datos y tecnología, la percepción pública y la expectativa de privacidad y los fundamentos políticos y legales que rodean esos datos. Su objetivo es lograr un equilibrio entre los derechos de privacidad individuales y al mismo tiempo permitir que los datos se utilicen con fines comerciales;
- **Privacidad de los datos:** la privacidad de la información es una rama de la seguridad de los datos relacionada con el manejo adecuado de los datos: consentimiento, notificación y obligaciones regulatorias. Más específicamente, preocupaciones prácticas de privacidad de datos: si o cómo se comparten los datos con terceros; cómo se recopilan o almacenan los datos legalmente y las restricciones regulatorias (por ejemplo, GDPR);
- **Seguridad de datos:** un conjunto de estándares y tecnologías que protegen los datos de la destrucción, modificación o divulgación intencional o accidental. La seguridad de los datos se puede aplicar utilizando una variedad de técnicas y tecnologías, que incluyen controles administrativos, seguridad física, controles lógicos, estándares organizacionales y otras técnicas de protección que se limitan a usuarios o procesos no autorizados o maliciosos;
- **Seguridad en Internet:** conocimiento a cerca de la seguridad personal del usuario y los riesgos en la información privada y propiedad asociada con el uso de Internet y la autoprotección contra el delito informático en general;
- **Malware:** cualquier programa o archivo que sea dañino para un usuario del ordenador. Los tipos de malware pueden incluir virus informáticos, gusanos, troyanos y *spyware*. Estos programas maliciosos pueden realizar una variedad de funciones diferentes, como robar, cifrar o eliminar datos confidenciales, alterar o secuestrar funciones informáticas centrales y monitorear la actividad del ordenador de los usuarios sin su permiso;
- **Phishing:** el *phishing* es una forma de fraude en el que un atacante se hace pasar por una entidad o persona de confianza en un correo electrónico u otros canales de

comunicación. El atacante usa correos electrónicos de *phishing* para distribuir enlaces maliciosos o archivos adjuntos que pueden realizar una variedad de funciones, incluida la extracción de credenciales de inicio de sesión o información de cuenta de las víctimas;

- **Violaciones de seguridad:** cualquier incidente que resulte en acceso no autorizado de datos, aplicaciones, servicios, redes y / o dispositivos al pasar por alto sus mecanismos de seguridad subyacentes. Una violación de seguridad ocurre cuando un individuo o una aplicación introduce ilegítimamente información privada, confidencial o no autorizada;
- **Spam:** sistemas de mensajería electrónica para enviar mensajes no solicitados o no deseados a granel. La forma más común de correo no deseado es el correo electrónico, pero el término también se aplica a cualquier mensaje enviado electrónicamente que no se haya solicitado y en masa;
- **Troyano:** tipo de *malware* que a menudo se disfraza de software legítimo. Puede ser empleado por ciber-ladrones y hackers que intentan acceder a los sistemas de los usuarios;
- **Virus:** el virus informático es un tipo de código o programa malicioso escrito para alterar la forma en que funciona un ordenador y está diseñado para propagarse de uno a otro.