enisa
European Network and Information Security Agency

Netz- und Informationssicherheit im pädagogischen Umfeld

Konsolidierter Beitrag der ENISA

Januar 2012

Danksagungen

Dieser Bericht ist das Ergebnis gemeinsamer Anstrengungen des luxemburgischen Ministeriums für Wirtschaft und Außenhandel und der ENISA. Die ENISA möchte Herrn Francois Thill, stellvertretender Direktor Kommunikation, und seinem Team für die offene und konstruktive Zusammenarbeit danken, die zu dieser Veröffentlichung geführt hat.

Über die ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist ein Kompetenzzentrum für Netz- und Informationssicherheit für die EU, ihre Mitgliedstaaten, den privaten Sektor und die europäischen Bürgerinnen und Bürger. Die ENISA entwickelt in Zusammenarbeit mit diesen Gruppen Ratschläge und Empfehlungen zu bewährten Verfahren im Bereich der Informationssicherheit. Sie unterstützt die EU-Mitgliedstaaten bei der Umsetzung einschlägiger EU-Rechtsvorschriften und arbeitet an der Verbesserung der Belastbarkeit der sensiblen Informationsinfrastrukturen und -netze in Europa. Die ENISA will die Fachkompetenz in den EU-Mitgliedstaaten durch die Entwicklung grenzüberschreitender Gemeinschaften fördern, die sich für die Verbesserung der Netz- und Informationssicherheit in der gesamten EU einsetzen. Weitere Informationen über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Kontaktangaben

Wenn Sie sich mit der ENISA in Verbindung setzen möchten oder allgemeine Fragen zur Informationssicherheit im pädagogischen Umfeld haben, verwenden Sie bitte die folgenden Kontaktangaben:

Daria Catalui, Netz- und Informationssicherheit in der Pädagogik, Stakeholder-Management, abgeordnete nationale Sachverständige, ENISA

E-Mail: daria.catalui@enisa.europa.eu

Louis Marinos, Senior Expert Risk Analysis & Management, ENISA

E-Mail: louis.marinos@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Impressum/Rechtshinweise

Inhalt

1 Zusammenfassung

Der Bericht zur Netz- und Informationssicherheit (NIS) im pädagogischen Umfeld erscheint in einer Zeit, in der Bildung, Pädagogik und Informationstechnologie mehr denn je miteinander verwoben sind. Die digital aktiven Bürger stehen vor der Herausforderung, sich über neue Entwicklungen im dynamischen Bereich der Informationstechnologie und insbesondere der Informationssicherheit auf dem Laufenden zu halten.

Lebenslanges Lernen, formale, nicht formale und informelle Bildung stehen auf der Agenda der politischen Entscheidungsträger. Kinder und Jugendliche sind ebenso wie ihre gleichaltrigen Bezugsgruppen, Eltern und Pädagogen Teil dieser Diskussion, und es wird empfohlen, dass sie im größtmöglichen Umfang zusammenarbeiten und sich einbringen.

Beim Thema Netz- und Informationssicherheit im pädagogischen Umfeld geht es um die Übermittlung grundlegender Sicherheitsinformationen an junge Internetnutzer.

Wir verfolgen damit das Ziel, den Wissenstransfer zwischen allen beteiligten Akteuren in Gang zu bringen, um nachhaltige Ergebnisse zu erzielen, die sich tatsächlich auf die europäischen digitalen Bürger auswirken. Eine Möglichkeit, dies zu erreichen, ist die Verbreitung der Arbeitsergebnisse der ENISA aus den letzten Jahren in einer für die Zielgruppe verständlichen Sprache. Wir haben die Ergebnisse der ENISA-Berichte in kurzen Übersichten zusammengefasst. Interessierte können dieses Material lesen und nutzen und bei Bedarf zu weiteren Einzelheiten die Dokumente im Volltext konsultieren. Die Berichte wurden nach Inhalten ausgesucht, die für pädagogische Zwecke relevant sind und direkt genutzt werden können.

Darüber hinaus möchten wir in diesem Bericht auf die ausgezeichnete Arbeit hinweisen, die verschiedene (nationale und internationale) Organisationen in diesem Bereich geleistet haben. Um auf dem neuesten Stand zu sein und die relevantesten Informationen zu verwenden, haben wir im Anhang unter „Verwandte Arbeiten“ einige Leseempfehlungen aufgenommen (siehe Anhang III: Verwandte Arbeiten).

In der Leitinitiative der Europäischen Kommission „Eine Digitale Agenda für Europa“[1] heißt es, *„Durch das Engagement der Jugend wird die Digitale Agenda Realität werden“*. Die Informationen in diesem konsolidierten Bericht tragen zur besseren Information, besseren Aufklärung und stärkeren Einbeziehung im Bereich der Netz- und Informationssicherheit bei und fördern somit die Ziele der Digitalen Agenda.

[1] *http://blogs.ec.europa.eu/neelie-kroes/youth-engagement-will-make-the-digital-agenda-a-reality/ (Stand: 25 Oktober 2011)*

2 Einleitung

Mit diesem Dokument soll eine konsolidierte Fassung der verfügbaren Ergebnisse der ENISA in einer Form vorgelegt werden, die für pädagogische Zwecke geeignet ist. Das Material wendet sich an Einrichtungen des Primarbereichs und insbesondere Pädagogen, Eltern und in gewissem Umfang auch Jugendliche.

Einschlägige Ergebnisse der ENISA sollten vereinfacht und in eine Form gebracht werden, die leicht für pädagogische Zwecke, die Ermittlung der erforderlichen Kompetenzen bzw. die direkte Verwendung durch einschlägige Akteure angepasst werden kann. Es geht uns nicht darum, das bestehende ausgezeichnete Material in diesem Bereich zu ersetzen, vielmehr wollten wir kurz gefasste Informationen über Arbeiten der ENISA vorlegen, die sich leicht in vorhandene pädagogische Materialien einbinden lassen. Der Text zu den im Folgenden aufgeführten Themen stammt aus einschlägigen Veröffentlichungen der ENISA.

Die vorliegende Arbeit ist das Ergebnis einer fruchtbaren Zusammenarbeit zwischen dem luxemburgischen Ministerium für Wirtschaft und Außenhandel und der ENISA: Ausgehend von der Struktur der vorliegenden pädagogischen Materialien der Mitgliedstaaten wurde das vorhandene Material der ENISA zusammengefasst und bearbeitet, damit die Mitgliedstaaten es nutzen können. Nach Rücksprache mit verschiedenen Akteuren haben wir eine Liste von Arbeiten der ENISA in folgenden Bereichen zusammengestellt:

- Cyber-Mobbing/Online-Grooming[2]
- Kinder in virtuellen Welten[3]
- Quiz zur Sensibilisierung[4]
- Leitlinien für Eltern, Erziehungsberechtigte und Pädagogen[5]
- Sicherheitsprobleme bei der Nutzung von Social-Networking-Internetseiten[6]
- Cookies[7]
- Sicherheitsprobleme in virtuellen Welten[8] und
- Sicheres Drucken[9]

---

[2] https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/

[3] http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds-what-parents-should-know-de

[4] http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-de

[5] http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians

[6] http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks

[7] http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies

[8] http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming

[9] http://www.enisa.europa.eu/activities/awareness-raising/deliverables/2008/secure-printing-de

Für diese Informationen wurde das folgende Format gewählt:

- eine kurze Beschreibung des Themas/Bereichs,
- Verweise auf die wichtigsten Ergebnisse/Empfehlungen,
- Verweis auf den Volltext und
- Folien, die für Präsentationen genutzt werden können.

Unser Ziel ist es, interessierte Akteure in die Lage zu versetzen, aus den konsolidierten Informationen Lernziele zu gewinnen und sie in ihre Konzepte einzubinden. Da wir davon ausgehen, dass die Informationen in diesem Bericht wiederverwendet und auf bestimmte pädagogische Anforderungen und vorhandene Methoden angepasst werden, hatte das Layout keine Priorität für uns.

Wir weisen darauf hin, dass das vorliegende Material eine Zusammenstellung einschlägiger Arbeiten der ENISA ist, die in den letzten drei bis vier Jahren durchgeführt wurden.

2.1 Zielgruppe

Wie im Arbeitsprogramm 2011[10] erwähnt, unterstützt die Agentur einen offenen mehrseitigen Dialog und pflegt aus diesem Grund enge Beziehungen mit der Industrie, dem wissenschaftlichen Sektor und den Nutzern. Daher wendet sich der Bericht an alle Interessengruppen, für die Fragen der Netz- und Informationssicherheit in der pädagogischen Arbeit von Bedeutung oder von Interesse sind.

Wie bereits erwähnt, richtet sich dieser Bericht an alle Personen, die mit der Bildung im Primarbereich befasst sind. Dazu gehören Eltern, Erziehungsberechtigte und Pädagogen, zuständige Behörden der Mitgliedstaaten (z.B. Ministerien, nationale Organisationen im pädagogischen Umfeld, Freiwilligenorganisationen, Interessengruppen usw.). Außerdem kann dieses Material auch von Jugendlichen selbst genutzt werden, damit sie Einblick in verschiedene Fragen der NIS in den genannten Bereichen gewinnen können.

[10] http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011/view *(Stand: 25. Oktober 2011)*

3 Verwandte Arbeiten

In den letzten Jahren wurde die Frage der NIS im pädagogischen Umfeld in verschiedenen Berichten und Artikeln angesprochen. Wir haben uns dafür entschieden, einige der Quellen zu zitieren, um einen allgemeinen Überblick über das vorhandene Material in diesem Bereich zu geben.

Abschlussbericht „EU kids online“[11] Aussagen über die notwendigen politischen Strategien in diesem Bereich

Dieser Bericht wurde von EU Kids online veröffentlicht. „EU Kids online verfolgt das Ziel, den Wissensstand über die Erfahrungen und Verfahrensweisen europäischer Kinder und Eltern in Bezug auf den gefährlichen und sichereren Umgang mit dem Internet und neuen Online-Technologien zu verbessern, um eine Informationsgrundlage für die Förderung eines sicheren Online-Umfelds für Kinder zu schaffen.“[11]. Es geht darin vor allem um folgende Themen:

- Wenn Kinder dazu angeregt werden, online stärker aktiv zu sein, verbessert das ihre digitalen Kompetenzen.
- Die Vermittlung von IT-Sicherheitskompetenzen verbessert wahrscheinlich auch andere Kompetenzen, während durch die Vermittlung instrumentaler und Informationskompetenzen auch die Sicherheitskompetenzen verbessert werden.
- Immer noch gibt es keine Chancengleichheit bei den digitalen Kompetenzen. Es müssen Anstrengungen unternommen werden, um die Ungleichheiten zu beseitigen.
- Unzureichende Kompetenzen bei jüngeren Kindern sind eine Priorität für Lehrkräfte und Eltern, da Kinder immer früher online gehen.
- Da die häufige Internetnutzung für viele Kinder in Europa inzwischen gängige Praxis ist, haben sich die politischen Prioritäten verändert. Für Kinder, die noch keinen Zugang haben, sollte unbedingt gewährleistet werden, dass der digitale Ausschluss nicht die soziale Ausgrenzung verstärkt. Für Kinder, die Zugang zu Internet haben, muss für eine ausreichende und angemessene Nutzungsqualität und -breite gesorgt werden.
- Die Anstrengungen zur Förderung der digitalen Bürgerschaft von Kindern – in Bezug auf Online-Sicherheit und bewährte Verfahren – tragen erste Früchte und sollten verstärkt werden.

[11] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf (Stand: 25. September 2011)

- Nicht nur die Eltern tragen Verantwortung für Kinder. Auch die Lehrkräfte spielen eine wesentliche Rolle, und für viele Kinder sind auch die Gleichaltrigen eine wertvolle Informationsquelle: 63 % der europäischen 9- bis 16-Jährigen werden von Eltern zur Internetsicherheit beraten, 58 % von Lehrkräften und 44 % von Gleichaltrigen.

Europäische Kommission: Schutz der Kinder in der digitalen Welt[12]

Dieses Dokument ist ein Bericht der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Anwendung der Empfehlung des Rates vom 24. September 1998 zum Jugendschutz und zum Schutz der Menschenwürde und der Empfehlung des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweiges der audiovisuellen Dienste und Online-Informationsdienste. Er enthält die folgende Aussage zum pädagogischen Umfeld:

- Initiativen zur Verbesserung der Medienkompetenz und zur Sensibilisierung werden teilweise in die formale Bildung integriert, wobei versucht wird, auch die Eltern und Lehrer zu sensibilisieren. Allerdings hat eine 2009 von der Kommission durchgeführte Untersuchung ergeben, dass dieses Thema in 23 europäischen Ländern zwar in den nationalen Lehrplänen steht, die tatsächliche Vermittlung derartiger Bildungsinhalte aber bruchstückhaft und uneinheitlich ist.

Forschungsarbeit der ITU[13]: Gezielte Maßnahmen für junge Menschen könnten große Veränderungen anstoßen

In einem Bericht über die Preise und die Verbreitung von IKT legt die ITU dar, dass sich die Verbreitung von Informations- und Kommunikationstechnologien (IKT), angetrieben durch das kontinuierliche Sinken der Preise für Telefon- und Internet-Breitbanddienste, weltweit weiter beschleunigen wird. In den Anmerkungen werden folgende Aussagen über junge Menschen gemacht.

- In dem Bericht „Measuring the Information Society 2011" (Messung der Informationsgesellschaft 2011) wird ausgeführt, dass die wichtigsten Barrieren für die Internetnutzung nicht immer auf Infrastruktur und Preis zurückzuführen sind. Erhebliche Unterschiede in den Nutzungsmustern hängen mit Bildungsstand, Geschlecht, Einkommen, Alter und Standort (ländliche oder städtische Gebiete) zusammen. So sind beispielsweise die Unterschiede zwischen den Internet- Nutzungsmustern von gut

---

[12] http://ec.europa.eu/avpolicy/reg/minors/rec/2011_report/index_de.htm *(Stand: September 2011)*

[13] http://www.itu.int/net/pressoffice/press_releases/2011/31.aspx *(Stand: 16.9.2011)*

ausgebildeten Personen mit hohem Einkommen in Entwicklungs- und Industrieländern bemerkenswert gering. Personen mit höherem Bildungsabschluss nutzen das Internet mehr als Menschen mit geringerem Bildungsniveau, und in den meisten Ländern sind mehr Männer als Frauen online.

- Junge Menschen (unter 25 Jahren) sind häufiger online als ältere, und die Internetnutzung von Personen, die sich noch in der Ausbildung befinden, ist intensiver als bei denjenigen, die keine Bildungseinrichtung mehr besuchen. Wenn man davon ausgeht, dass das Internet auch weiter genutzt wird, wenn sich die Nutzer daran gewöhnt haben, online zu sein, werden die Schüler und Studierenden von heute mit größerer Wahrscheinlichkeit künftige Internetnutzer. Für junge Menschen in der ganzen Welt sind soziale Netzwerke und nutzergenerierte Inhalte, wie z. B. Blogs, entscheidende Faktoren für die Verbreitung des Internets.

- Da 46 % der Bevölkerung in den Entwicklungsländern (über 2,5 Milliarden Menschen) unter 25 Jahre alt sind, wird in dem Bericht als eine der wirksamsten Möglichkeiten zur Steigerung der Internetnutzung in diesen Ländern vorgeschlagen, gezielt die jüngere Generation anzusprechen – z. B. durch die Anbindung von Schulen und anderen Bildungseinrichtungen und die Erhöhung der Bildungsbeteiligung.

***The great schools revolution (Die große Schulrevolution), The Economist*[14]**

In einem Artikel zur Bildungsreform in der Wochenzeitschrift The Economist geht es um Fragen der künftigen Ausrichtung der Bildung, bei denen auch die Rolle der neuen Technologien und die Kompetenzen der Kinder eine Rolle spielen.

- Auch die Technologie hat spürbare Auswirkungen. Nach einer Reihe von Fehlstarts glauben inzwischen viele Menschen, dass das Internet einen erheblichen Beitrag zur Bildung der Kinder leisten kann. Die für Arbeitnehmer zunehmende Notwendigkeit, ihre Kompetenzen auf den neuesten Stand zu bringen und anzupassen, ist eines der Themen des neuen Buches „The Shift: The Future of Work is Already Here“ (Der Übergang: Die Zukunft der Arbeit hat schon begonnen) von Lynda Gratton von der London Business School. Sie argumentiert, dass die Geschwindigkeit des Wandels so hoch sein wird, dass die Menschen unter Umständen alle paar Jahre neue Fachkompetenzen erwerben müssen, wenn sie sich auf dem lukrativen Markt für gesuchte Talente halten wollen. Sie

[14] *http://www.economist.com/node/21529014?fsrc=nlw|edh|09-15-11|editors_highlights (Stand: 17 September 2011)*

nennt diesen Prozess „serial mastery“ (serielle Meisterschaft) und stellt fest, dass das derzeitige Bildungssystem in den meisten Ländern, vom Kindergarten bis zur Universität, die Menschen schlecht auf das kontinuierliche Lernen vorbereitet. Wahrscheinlich wird es in der Weiterbildung, vor allem online, eine Innovationswelle geben, die diesem Bedarf auf flexiblere, individuellere Weise gerecht wird als traditionelle Studiengänge der verschiedenen Stufen.

- Die Mitgliedstaaten stimmen zwar darin überein, dass die Förderung von Selbstregulierungsmaßnahmen (Verhaltenskodizes) nützlich ist, doch es bestehen weiterhin Bedenken, dass die Schutzniveaus in diesem Bereich immer noch erhebliche Unterschiede aufweisen. Künftig sollten bestehende Maßnahmen gegen illegale oder schädliche Inhalte laufend überwacht werden, um ihre Wirksamkeit zu gewährleisten. So entstehen z. B. Stellen der Inhaltsanbieter, bei denen Kinder und Eltern derartige Inhalte melden können, unterstützt von einer funktionierenden Backoffice-Infrastruktur, doch all diesen Initiativen fehlen gemeinsame Merkmale und Skaleneffekte, mit denen ihre Effizienz gesteigert werden könnte.

4 ENISA-Materialien in Kurzfassung

Im Folgenden geben wir Übersichten zu den ermittelten Bereichen der NIS, die für pädagogische Zwecke relevant sind. Bitte beachten Sie, dass die folgenden Ausführungen in den meisten Fällen direkt den entsprechenden Berichten der ENISA entnommen sind. Wir empfehlen Ihnen, für detailliertere Informationen die ENISA-Berichte zu konsultieren.

4.1 Cyber-Mobbing und Online-Grooming: Hilfe beim Schutz gegen Risiken

Kinder sind – unabhängig von ihrer Kultur, Religion und nationalen Herkunft – der wertvollste Teil jeder Gesellschaft. Sie sind auf die Fürsorge ihrer Eltern, der Schule und ihres sozialen Umfelds angewiesen. Aufgrund ihrer Fürsorgepflicht bereiten den Eltern Aktivitäten ihrer Kinder Sorge, die gefährlich sein könnten, wie z. B. Extremsportarten oder die Nutzung von Technologie. Das letztere Thema ist für Eltern besonders besorgniserregend, das sie mit der Technologie nicht so unbefangen umgehen wie ihre Kinder, die:

- Spaß beim Umgang mit Technologie/Gadgets haben
- Technologie intuitiv nutzen
- sehr leicht Verständnis für die Nutzung technischer Funktionen entwickeln
- sehr vertraut mit Innovationen werden
- IKT als Lerninstrument nutzen
- Technologie verwenden, um mit ihren Freunden zu kommunizieren.

Was sind Mobbing und Grooming?

Eine Definition beschreibt das Mobbing anhand seiner negativen Auswirkungen auf das Opfer und sieht es als negative und schädliche Behandlung anderer Menschen in einer Form, die dazu führt, dass die Zielperson leidet und sich gedemütigt oder verletzlich fühlt und die sich schädlich und belastend auf diese Person auswirkt. Wie die Belästigung wird auch das Mobbing weitgehend anhand der Auswirkungen des Verhaltens auf die Zielperson, nicht der Absicht, definiert. Mobbing kann deshalb vorwiegend als Aggression oder andauernde physische oder psychische Gewalt definiert werden, die von einer Einzelperson oder Gruppe ausgeübt wird und gegen eine Person gerichtet ist, die sich in dieser Situation nicht verteidigen kann.

Ziel des Grooming ist die Vorbereitung eines Opfers. Grooming dient der Auswahl eines Opfers, um festzustellen, ob diese Person aufgrund des Machtungleichgewichts und des Zwangs bei sexuellem Missbrauch kooperieren könnte. Durch Grooming soll erreicht werden, dass sich das potenzielle Opfer sicher genug fühlt, um sich einem Straftäter zu nähern, mit ihm allein zu sein und dessen Verhalten nach dem MISSBRAUCH geheim zu halten.

Empfehlungen

Die ENISA hat Empfehlungen zur Minderung der Risiken veröffentlicht, denen junge Menschen im Cyberspace ausgesetzt sind. Die Empfehlungen sind nach den betroffenen Gruppen in verschiedene Kategorien eingeteilt:

Was sollten Eltern/Erziehungsberechtigte/Lehrkräfte und Erzieher tun?

- BESSERE INFORMATION ÜBER VERHALTENSWEISEN: Bessere Information von Eltern und Pädagogen über die Online-Verhaltensmuster von Minderjährigen. Laufende Kommunikation mit Eltern/Pädagogen. Gespräche über Unregelmäßigkeiten und Hinzuziehung von einschlägigen Fachleuten (Verhaltenpsychologen) und Wissensaustausch in diesem Bereich.

- BESSERE INFORMATION ÜBER TECHNISCHE FRAGEN: Vermittlung von Wissen zu technischen Fragen an Eltern/Pädagogen. Je nach ihrer Rolle in der Fürsorge/Erziehung und Bildung ist jeweils ein unterschiedlicher Wissensstand erforderlich.

- KLARERE HALTUNG ZUR PRIVATSPHÄRE: Jugendliche, Eltern und Pädagogen sollten über Fragen der Privatsphäre in Bezug auf die Cyberwelt informiert sein.

- WISSENSAUSTAUSCH ANSTOSSEN: Eltern und Minderjährige sollten regelmäßig technisches Wissen austauschen. Wenn in technischen Fragen ein offener Kanal zu den Jugendlichen besteht, ist es einfacher, ihre Kenntnisse, ihr Interesse, den Umfang und die Muster ihrer Nutzung einzuschätzen.

- EINSATZ SPEZIELLER SICHERHEITSEINSTELLUNGEN FÜR ELTERN/PÄDAGOGEN: Es sollte der Einsatz von Sicherheitseinstellungen erwogen werden, die speziell für den Gebrauch von Eltern/Pädagogen angepasst sind.

- UNTERSTÜTZUNG FÜR JUGENDLICHE IN DER SCHULE: Es ist wichtig, potenzielle Cyber-Mobbing- und Online-Grooming-Angriffe so früh wie möglich zu ermitteln. Deshalb sollten Jugendliche direkten Zugang zu spezialisierten Beratungsstellen in den Schulen haben, an die sie sich wenden können, wenn sie Unterstützung brauchen.

Was sollten Jugendliche tun?

- EINSATZ SPEZIELLER SICHERHEITSEINSTELLUNGEN FÜR JUGENDLICHE: Den Einsatz von Sicherheitseinstellungen für von Jugendlichen verwendeten Geräten erwägen, um einen einfachen Zugang zu Informationen zu verhindern.

- ANPASSUNG BEREITS EXISTIERENDER SICHERHEITSEINSTELLUNGEN AN DIE BEDÜRFNISSE VON JUGENDLICHEN: In vielen Bereichen des täglichen Lebens gibt es heutzutage Sicherheitseinstellungen, die an die Bedürfnisse von Kindern angepasst sind (z. B. in Autos, Flugzeugen, Schiffen, bei Spielzeugen usw.). Ein ähnlicher Ansatz sollte auch im Cyberspace angewandt werden. Wir empfehlen deshalb die Einführung von speziell für Jugendliche/Minderjährige maßgeschneiderten Sicherheitseinstellungen.

- ENTWICKLUNG VON ONLINE-RATING-SYSTEMEN: In der Fernseh- und Filmindustrie gibt es Eltern-Leitlinien zur Bewertung von Fernsehsendungen im Hinblick auf sexuell eindeutige Inhalte, unverblümte Gewalt und Obszönität. Im Bereich der Computer- und Videospiele existieren ähnliche Leitlinien für eine entsprechende Bewertung/Klassifizierung. In ähnlicher Form könnte die Festlegung von Eltern-Leitlinien für Online-Inhalte (Dienste, Websites, Social Networking-Anwendungen usw.) erwogen werden.

- DATENSCHUTZ-FOLGENABSCHÄTZUNGEN: Zahlreiche Internet-Anwendungen/-Dienste verarbeiten erhebliche Mengen personenbezogener Daten (z. B. Social-Networking-Seiten). Es wird empfohlen, Kriterien zu entwickeln, um Anwendungsgebiete zu ermitteln, in denen vor Einführung des Dienstes eine Datenschutz-Folgenabschätzung durchgeführt werden muss.

- DEAKTIVIERUNG ALLER AKTIVEN KOMPONENTEN: Auf verschiedenen Handgeräten, tragbaren Computern usw. können Anwendungen installiert sein, die aktive Komponenten beinhalten, also Daten (z. B. Standortdaten, Bewegungsdaten usw.) im Hintergrund übermitteln/verarbeiten. Wir empfehlen, dass den Nutzern Funktionen zur Verfügung gestellt werden, mit denen sie alle Hintergrundfunktionen abschalten können, die personenbezogene Daten an Dienst-/Anwendungsanbieter übermitteln.

- VERBESSERUNG ALTERSGEMÄSSER ZUGANGSKONTROLLMECHANISMEN: Wir empfehlen, dass das Alter der Nutzer in der gesamten Infrastruktur und insbesondere bei den Authentifizierungs-/Autorisierungsmechanismen ein fester Bestandteil ihrer Anmeldedaten wird.

Zur Abschätzung der Risiken haben wir das Szenario „Kristie online“ verwendet. Einzelheiten dazu sind im ENISA-Bericht beschrieben.

Weitere Informationen finden Sie unter:

https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/

4.2 Kinder in virtuellen Welten: Was Eltern wissen sollten

Jeden Tag scheint eine neue Social-Networking-Website im Internet zu entstehen. Die Online-Nutzer haben die Qual der Wahl zwischen Facebook und Bebo, MySpace und Second Life bis hin zu kommerziell ausgerichteten Angeboten wie LinkedIn. Mittlerweile hat sich jedoch ein neues, wachsendes Internet-Phänomen entwickelt, das sich an die jüngere Generation richtet. Die größte Sorge in Bezug auf virtuelle Welten ist die Online-Sicherheit von Kindern (bis zu 7 Jahren) und Tweens (8 bis 12 Jahre) und die Frage, wie sie vor Online-Verbrechern geschützt werden können. Erwachsene müssen die Kinder unterstützen, um positive Erfahrungen in diesen dreidimensionalen Umgebungen sicherzustellen.

Eltern sind natürlich besorgt darüber, wie sich ihre Kinder in den virtuellen Welten verhalten und diese nutzen. Es werden Informationen benötigt, um Eltern in die Lage zu versetzen, gemeinsam mit ihren Kindern zu entscheiden, was angemessen und sicher ist und wie man sich in den virtuellen Welten verantwortungsbewusst verhält.

Was sind virtuelle Welten?

Virtuelle Welten sind computergestützte simulierte Umgebungen, die von Nutzern bewohnt werden und in denen diese über Avatare interagieren. Avatare sind normalerweise textuelle, zwei- oder dreidimensionale grafische Darstellungen; es sind jedoch auch andere Formen (z. B. akustische und Tastempfindungen) denkbar. Einige virtuelle Welten ermöglichen die Nutzung durch mehrere Personen.

Der Computer greift auf eine computersimulierte Welt zu und bietet dem Nutzer Wahrnehmungsreize, der wiederum Elemente der Modellwelt manipulieren kann und so eine gewisse Telepräsenz erfährt. Derartige Modellwelten können der realen Welt ähneln oder Fantasiewelten darstellen. Die Modellwelt kann Regeln simulieren, die auf denjenigen der realen Welt oder einer Hybrid-Fantasiewelt basieren. Beispiele für solche Regeln sind Schwerkraft, Topografie, Fortbewegung, Echtzeithandlungen und Kommunikation.

Warum betreten Kinder virtuelle Welten?

Junge Menschen betreten virtuelle Welten im Internet aus verschiedenen Gründen, u. a. um:

- mit Freunden in einer neuen Umgebung und in Echtzeit zu interagieren sowie gemeinsamen Interessen nachzugehen;
- Communities (Gemeinschaften) oder Interessengruppen, z. B. zu Musik, Fußball usw. zu gründen und ihnen beizutreten;
- Gedanken und Informationen über Interessensgebiete über Blogs, Instant Messaging (sofortige Nachrichtenübermittlung) und andere Tools auszutauschen;

- neue Leute zu treffen und letztlich neue Freundschaften zu schließen;
- originäre und persönliche Inhalte wie Bilder, Fotos und Videos zu erzeugen und auszutauschen, um die Möglichkeiten der Selbstdarstellung zu erweitern;
- Musik zu erzeugen, zu veröffentlichen und auszutauschen;
- Spiele zu spielen;
- einen eigenen Raum zu haben, selbst wenn Eltern und Betreuungspersonen anwesend sind;
- mit der eigenen Identität zu experimentieren, neue soziale Räume und Grenzen auszuprobieren.

Berichte und Auswertungen der ENISA stellen vier Hauptprobleme heraus:

- Mobbing
- Belästigung
- illegale Inhalte
- Kindesmissbrauch.

Zudem erhöhen sich die Risiken durch:

- unsichere Umgebungen
- fehlende pädagogische Inhalte
- Produktplatzierung in virtuellen Welten
- auf Kinder ausgerichtete Werbung
- Kosten für die Nutzung
    - monatliche Gebühren
    - Kauf von Produkten
    - Werbung.

Wie können Eltern und Betreuungspersonen Kinder unterstützen?

- Lesen Sie vor dem Betreten einer virtuellen Welt gemeinsam mit Ihren Kindern die Nutzungsbedingungen, diskutieren Sie Sicherheitsmaßnahmen, stellen Sie einige Grundregeln auf und überwachen Sie die Nutzung, um die Einhaltung der Regeln zu gewährleisten.
- Klären Sie junge Nutzer über die verantwortungsvolle Nutzung von Technologie allgemein auf und ermutigen Sie sie, ihren Instinkten zu vertrauen und gesunden Menschenverstand einzusetzen.
- Sorgen Sie für den Einsatz u. a. folgender technischer Lösungen:
    - Filter und elterliche Kontrollen;
    - Nutzungsverlauf;
    - Bestätigung der Nutzung einer automatischen Moderation, z. B. von Textfiltern, die bestimmte Wortmuster und URL erkennen, oder von komplexeren Filtern wie Anti-Grooming-Engines (AGE);
    - „Ratings“ (Bewertungen): Eltern und Betreuungspersonen sollten Rating-Symbole und ihre Verwendung kennen. Mit diesem wichtigen Tool können junge Nutzer vor unangemessenen Diensten und Inhalten geschützt werden;
    - Altersüberprüfung.
- Überprüfen Sie, ob die virtuelle Welt durch aktive Moderation („in game“: innerhalb des Spiels und/oder „silent“: „stumm“) überwacht wird.
- Nehmen Sie Anteil an den Aktivitäten der jungen Nutzer in der virtuellen Welt.
- Bleiben Sie gelassen und ziehen Sie keine voreiligen Schlüsse, wenn Sie etwas hören oder sehen, was Sie in Bezug auf das Verhalten Ihres Kindes oder das Verhaltens seiner Online-Freunde besorgt. Wenn Ihre Kinder befürchten müssen, dass Sie sie von ihren sozialen Lebensadern einfach abschneiden, werden sie wahrscheinlich nur immer unwilliger ihre möglichen Probleme und Sorgen mitteilen.
- Seien Sie Berichten der Virtual-World-Community-Teams gegenüber offen, dass sich Ihr Kind online möglicherweise vollkommen anders verhält als offline mit Ihnen im persönlichen Kontakt.

- Lernen Sie die Online-Kultur kennen, sodass Sie die typischen Entschuldigungen junger Leute durchschauen, wenn sie für ihr Online-Verhalten Verantwortung übernehmen sollen, z. B. „Jemand hat meinen Account gestohlen“.
- Vermitteln Sie Ihren Kindern, ihre Passwörter für den Zugang zu der virtuellen Welt nicht ihren Freunden oder Geschwistern mitzuteilen.
- Wenden Sie sich über die Kontakt-Seite der Virtual-World-Website an den Leiter/die Leiterin der Community und teilen Sie ihnen Ihre Sorgen und Fragen mit.
- Gehen Sie nicht davon aus, dass es jeder und jede im Netz auf Ihr Kind abgesehen hat. Die Statistiken belegen, dass Probleme mit Pädophilen in der Realität weit häufiger sind als im Internet. Im Allgemeinen sind Websites für Kinder sicher und können eine wunderbare, kreative, sozial und pädagogisch wertvolle Erfahrung für Ihr Kind darstellen – aber nur, wenn Sie engagiert und wachsam bleiben.

Zur weiteren Verbreitung der oben aufgeführten Informationen hat die ENISA ein Plakat mit 10 Internet-Tipps für Eltern und Erziehungsberechtigte veröffentlicht (siehe das Plakat, das Sie gern verwenden können).

Weitere Informationen finden Sie unter:

http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds-what-parents-should-know-de

4.3 Quiz-Vorlagen zur Schärfung des Bewusstseins für Informationssicherheit

Worum geht es in dem Quiz?

Die Quiz-Vorlagen sollen den Teilnehmenden eine Vorstellung davon vermitteln, wie bewusst ihnen die Vorteile und Gefahren der Nutzung von Computern und Online-Diensten im Internet sind und hoffentlich ihr Interesse an diesen Fragen steigern. Sie sollen also nicht als Instrument angesehen werden, mit dem Einzelpersonen im Selbsttest ihr jeweiliges Sensibilisierungs- und Kenntnisniveau genauestens erfassen, sondern die Aufmerksamkeit in die richtige Richtung lenken und die Themen herausstellen, deren Weiterbearbeitung zur Steigerung des Sicherheitsbewusstseins lohnt. Zielgruppen dieser Arbeit der ENISA sind Eltern, Endbenutzer und kleine und mittlere Unternehmen (KMU).

Diese Materialien liegen in verschiedenen Sprachen (EN, ES, DE, FR, IT, DA, PL) vor und sind somit für viele potenzielle Nutzer attraktiv.

Aufgrund des Umfangs der Quiz-Vorlagen geben wir im Folgenden lediglich einen Überblick über das Eltern-Quiz und legen allen Interessierten nahe, sich anhand der hierzu interessanten Teile des ENISA-Bericht (S. 13-21) genauer zu informieren. Wir gehen davon aus, dass sich diese Teile direkt weiterverwenden lassen, da sie allgemein und umfassend sind.

Überblick über das Eltern-Quiz

Im Zusammenhang mit der NIS im pädagogischen Umfeld ist der Teil der Quiz-Vorlagen, der sich an Eltern richtet, von besonderem Interesse. Mit diesem Quiz können Eltern ihr Bewusstsein und ihr Wissen in Fragen der Computer- und Internet-Nutzung Ihres Kindes testen. Es kann dazu beitragen, ihr Interesse an den Vorteilen und Gefahren der Internetnutzung durch ihr Kind zu steigern.

Das Eltern-Quiz deckt folgende Bereiche ab: PC-Nutzung durch Kinder, Privatsphäre & soziale Netzwerke, illegale Inhalte, Filesharing und Cyber-Mobbing.

Weitere Einzelheiten und das Quiz für Endbenutzer finden Sie unter:

http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-de

4.4 „Guidelines for Parents, Guardians and Educators“ (Leitlinien für Eltern, Erziehungsberechtigte und Pädagogen) Bericht der ITU in Zusammenarbeit mit der ENISA

Finden Sie heraus, welche Art von Online-Erfahrung Ihr Kind sucht

Das Internet hat ein großes Potenzial als Instrument, mit dem Kinder und Jugendliche selbstständig Hilfe und Informationen finden können. Stützen Sie das Lernen auf emotionale Erfahrungen, ein entscheidendes Ziel besteht darin, positive und verantwortliche Online-Verhaltensweisen zu vermitteln. Dabei sollten Sie verstehen, welche Art von Online-Erfahrung Ihr Kind vermutlich sucht (siehe S. 12-13 des Berichts). Diese Information ist ein entscheidender Faktor dafür, welchen Risiken Kinder ausgesetzt sind und welchen Schutz sie folglich benötigen.

Was viele Eltern, Erziehungsberechtigte und Pädagogen nicht wissen:

Aktuelle Untersuchungen der ENISA haben gezeigt, dass in den meisten Fällen Eltern oder Erziehungsberechtigte über die wahrscheinlichen Erfahrungen ihrer Kinder im Internet und die Risiken und Gefahren verschiedener Online-Aktivitäten nicht im Einzelnen informiert sind. Kinder können über verschiedene Plattformen und Geräte online gehen, u. a.:

- Personalcomputer (PC)
- Mobiltelefone
- persönliche digitale Assistenten (PDA).

Welche Rolle kommt den Pädagogen zu?

Es ist sehr wichtig, dass Pädagogen keine Mutmaßungen darüber anstellen, was Kinder und Jugendliche über Internetsicherheit wissen oder nicht wissen. Es kursieren viele falsche Vorstellungen über das Internet und darüber, welches Verhalten angemessen oder unangemessen ist. So verraten sich viele Teenager gegenseitig ihre Passwörter, was oft als Zeichen echter Freundschaft angesehen wird. Eine wichtige Aufgabe der Pädagogen ist es, Kindern und Jugendlichen zu vermitteln, wie wichtig Passwörter sind, wie man sie sicher schützt und wie man ein starkes Passwort erstellt. Ähnlich ist es bei Fragen des Urheberrechts: Viele Erwachsene sind entsetzt darüber, dass jüngere Nutzer anscheinend keine Bedenken haben, illegal Musik oder Videos herunterzuladen. Kinder und Jugendliche haben gewaltige Wissenslücken in Fragen der Legalität urheberrechtlich geschützter Inhalte im Internet. Auch hier haben Pädagogen ganz klar die Aufgabe, dies Kindern zu erklären. Die Schulen haben die Chance, mit IKT die Bildung zu verändern und den Schülern zu helfen, damit sie sowohl ihr Potenzial ausschöpfen als auch den Standard verbessern können. Wichtig ist jedoch auch, dass Kinder lernen, sich sicherheitsbewusst zu verhalten, wenn sie diese

neuen Technologien, besonders die kooperativen Technologien des Web 2.0, wie z. B. Social-Networking-Websites nutzen, die zunehmend ein zentraler Aspekt des produktiven und kreativen sozialen Lernens werden. Pädagogen können Kindern helfen, Technologien intelligent und sicher zu nutzen, indem sie:

- sicherstellen, dass die Schule über solide Richtlinien und Verfahren verfügt und dass deren Wirksamkeit regelmäßig überprüft und bewertet wird;
- sicherstellen, dass alle über die Nutzungsrichtlinien und ihre Nutzung informiert sind. Wichtig ist, dass die Nutzungsrichtlinien altersgemäß sind;
- überprüfen, ob in den Anti-Mobbing-Richtlinien der Schule auch auf Mobbing im Internet oder über Mobiltelefone oder andere Geräte erwähnt sind und wirksame Sanktionen bei Zuwiderhandlungen vorgesehen sind;
- einen Koordinator für Internetsicherheit ernennen;
- sicherstellen, dass das Computernetz der Schule sicher und geschützt ist;
- sicherstellen, dass ein akkreditierter Internet-Provider genutzt wird;
- eine Filter-/Überwachungssoftware einsetzen;
- alle Schüler in Internetsicherheit schulen und festlegen, wo, wie und wann diese Inhalte vermittelt werden;
- dafür sorgen, dass alle Mitarbeiter (einschließlich der Hilfskräfte) angemessen geschult und regelmäßig auf den neuesten Stand gebracht werden;
- für eine einheitliche Anlaufstelle in der Schule sorgen und in der Lage sind, Sicherheitsverletzungen zu dokumentieren, damit die Schule sich ein besseres Bild von Problemen oder Entwicklungen machen kann, die Maßnahmen erforderlich machen;
- sicherstellen, dass das Leitungsteam und der Schulverwaltungsrat sich der Probleme der Internetsicherheit bewusst sind;
- alle Internet-Sicherheitsmaßnahmen regelmäßig überprüfen lassen.

Was macht ein sicheres IKT-Umfeld aus?

Die Schaffung einer sicheren IKT-Lernumgebung erfordert verschiedene wichtige Elemente, wie z. B.:

- Aufgaben, Richtlinien und Verfahren
- ein wirksames Spektrum technologischer Instrumente
- ein umfangreiches Programm zur Internet-Sicherheitserziehung für alle Personen in der Einrichtung
- einen kontinuierlichen Überprüfungsprozess zur Überwachung seiner Wirksamkeit.

Daher ist es von zentraler Bedeutung, dass Eltern in der Lage sind, gemeinsam mit ihrem Kind zu entscheiden, welche Form der Nutzung angemessen und sicher ist und wie man sich in den virtuellen Welten verantwortungsvoll verhält. Wenn sie zusammenarbeiten, können Eltern, Pädagogen und Kinder die Vorteile von IKT nutzen und gleichzeitig die möglichen Gefahren für Kinder auf ein Mindestmaß reduzieren.

Weitere Informationen finden Sie unter:

http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians

4.5 Sicherheitsprobleme und Empfehlungen für Social-Networking-Internetseiten

Welche Schwachstellen haben soziale Netzwerke?

Soziale Netzwerke oder Social-Networking-Internetseiten (SNS) gehören zu den bemerkenswertesten technischen Phänomenen des 21. Jahrhunderts; einige SNS sind heute die weltweit am häufigsten aufgerufenen Websites.

Die Wirkung von Cyber-Stalking und Cyber-Mobbing auf die Opfer ist bekannt und kann von leichter Einschüchterung und Verlust der Privatsphäre bis zu ernsthaften körperlichen Verletzungen und psychischen Schäden reichen. Verschiedene Faktoren machen SNS besonders anfällig dafür, auf diese Art ausgenutzt zu werden.

- Viele Schulen verbieten die Benutzung von SNS in der Schule, was die Schüler stark davon abschreckt, Mobbing zu melden.
- Es ist einfach (mit einem gefälschten Profil) anonym zu bleiben.
- Es ist einfach, mit eingeschränkten Personengruppen zu kommunizieren (eine Funktion, die sehr nützlich ist, wenn sie zum richtigen Zweck genutzt wird).
- Soziale Netzwerke wirken als zentrale Plattform. SNS bieten alle üblichen Instrumente und Angriffsmöglichkeiten, die Cyber-Mobber nutzen, und noch mehr in einer einzigen Schnittstelle (Instant Messaging, mobiles Messaging, gefälschte Profile und Verleumdung usw.). Eltern und Erwachsene können oft nicht eingreifen, weil sie sich mit der verwendeten Technologie nicht auskennen.

In SNS mögliche Formen von Cyber-Mobbing

Verschiedene Arten von Aktivitäten können als eine Form des Cyber-Mobbing betrachtet werden. Eine frühzeitige Ermittlung dieser Verhaltensweisen kann dazu führen, dass negative Auswirkungen auf die Opfer wirksam aufgedeckt werden.

- Flaming: Online-Auseinandersetzungen mittels elektronischer Nachrichten mit aggressiver und vulgärer Ausdrucksweise
- Belästigung: Beispielsweise die wiederholte Versendung verletzender oder grausamer und beleidigender Nachrichten; die Erschleichung des Zugangs zum Nutzernamen und Passwort einer anderen Person, um unangemessene Nachrichten an die Listen von Freunden zu schicken

- Verunglimpfung: Einrichtung von Accounts unter dem Namen anderer Personen, um diese zu erniedrigen; Verbreitung oder Veröffentlichung von Klatsch oder Gerüchten über eine Person, um ihren Ruf oder ihre Freundschaften zu schädigen; z. B. die Einrichtung von „Hass“-Websites, die Veröffentlichung von Witzen, Cartoons, Klatsch und Gerüchten, die sich alle gegen ein bestimmtes Opfer richten; Veröffentlichung schädigender, unwahrer und/oder grausamer Aussagen oder Bilder und Aufforderung an andere, dasselbe zu tun oder es zu kommentieren

- Aneignung einer anderen Identität: Vorgeben, eine andere Person zu sein und Versendung oder Veröffentlichung von Material, um diese Person in Schwierigkeiten oder in Gefahr zu bringen oder ihren Ruf oder ihre Freundschaften zu gefährden

- Outing: Verbreitung der Geheimnisse einer anderen Person oder Veröffentlichung peinlicher Informationen oder Bilder im Internet

- Tricks: Überredung anderer zur Offenlegung von Geheimnissen oder peinlichen Informationen, die dann online verbreitet werden

- Ausschluss: Ausschluss einer Person aus einer Online-Gruppe mit Absicht und aus niederen Beweggründen, z. B. wenn eine Online-Gruppe beschließt, eine bestimmte Person zur Strafe zu ignorieren

- Stalking: Intensive Belästigung und Verunglimpfung – in der Regel im Zusammenhang mit einer problematischen intimen Beziehung –, die Drohungen beinhaltet oder erhebliche Angst auslöst

- Drohendes Verhalten, direkt oder indirekt.

Dem Verbot von SNS in Schulen entgegenwirken

Immer mehr Schulen verbieten die Nutzung von SNS in der Schule oder schränken sie ein. Es wird empfohlen, dass Schulen und Entscheidungsträger im Bildungswesen die Folgen eines SNS-Verbots bedenken, da ein Verbot davon abschreckt, Mobbing zu melden. Zudem führt dies dazu, dass Eltern und Lehrkräfte mit geringerer Wahrscheinlichkeit die notwendigen Kompetenzen für eine Überwachung junger Menschen in diesem Bereich erwerben. So geht letztendlich eine wertvolle Bildungsressource verloren.

SNS sollten kontrolliert und offen genutzt (d. h. nicht verboten oder verteufelt) werden und es sollten koordinierte Kampagnen zur Aufklärung von Kindern, Lehrkräften und Eltern stattfinden.

Nicht die Technologien selbst sind für Mobbing verantwortlich, sondern die Personen, die sie missbrauchen. Deshalb sind die Bildung, die Vorbildfunktion einer positiven Technologienutzung durch Gleichaltrige und Erwachsene und die Selbstregulierung der Gemeinschaft entscheidende Faktoren für die Bekämpfung des Online-Mobbing.

Weitere Informationen finden Sie unter:

http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks

4.6 Cookies

Cookies – was ist das?

Cookies sind kleine Informationseinheiten, die auf dem PC eines Nutzers gespeichert und vielfach von Internet-Dienstanbietern genutzt werden, um ihre Dienste auszuführen, Präferenzen der Nutzer (Sprache, Layout, Benutzernamen usw.), Kennungen für Einkaufslisten in Online-Shops usw. zu erfassen Jede Website kann Cookies erzeugen, die auf den Rechnern der Nutzer gespeichert werden. Alle Aktivitäten im Zusammenhang mit der Speicherung und Übermittlung der Cookies sind für den Nutzer unsichtbar und werden von der besuchten Website gesteuert.

Welche Vorteile hat die Nutzung von Cookies?

Die Funktion von Cookies ermöglicht eine Nutzung zu folgenden Zwecken:

- Identifizierung und Authentifizierung von Nutzern (d. h. Vermeidung einer erneuten Identifizierung)
- Statistiken über Besuche, z. B. Websites, Zahl der Besuche usw.
- Speicherung von Präferenzen und Einstellungen.

Für Marketing und der Online-Werbung können sie zu folgenden Zwecken genutzt werden:

- Quantifizierung/Bewertung der Wirksamkeit von Werbung (d. h. Ermittlung der Zahl der Besucher (Unique Users), die als unmittelbare Reaktion auf eine Werbeanzeige eine Site besucht haben)
- Erstellung von Nutzerprofilen und ihre Verwendung für gezielte Werbung (d. h. Verhaltens-Targeting)
- bessere Steuerung von Werbeanzeigen (Anpassung an ein Nutzerprofil, Rotation und Vermeidung von Überschneidungen).

Welche Sicherheitsbedenken bestehen?

Die Sicherheitsbedenken in Bezug auf Cookies beziehen sich auf Fragen der Privatsphäre der Nutzer und häufige Angriffe auf der Grundlage der in Cookies enthaltenen Informationen.

- Sammlung privater Informationen zu Präferenzen der Nutzer, besuchten Websites, Statistiken
- Änderung von Informationen (z. B. Suchergebnissen)

- Böswilliges Einloggen in Accounts anderer Nutzer unter falscher Identität (z. B. Banking, E-Mail usw.).

Weitere Informationen finden Sie unter:

http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies

4.7 Virtuelle Welten – echtes Geld

Worum geht es bei der Sicherheit in virtuellen Welten?

Betrug im Online-Gaming (und in virtuellen Welten) ist der Missbrauch von Nutzerinformationen im Zusammenhang mit Online-Spielen. Bei solchen betrügerischen Aktivitäten zielen geht es um echtes Geld. Möglich werden sie durch den zunehmenden Einsatz von Schadprogrammen, die speziell auf Online-Spiele und virtuelle Welten ausgerichtet sind, und durch Tausende neuer Programme zum Diebstahl von Passwörtern von Online-Spielen.

Ziel der Angreifer ist es, virtuelle Objekte und virtuelles Eigentum zu stehlen und auf einem existierenden bzw. entstehenden grauen Markt weiterzuverkaufen.

Was sind die fünf wichtigsten Risiken in virtuellen Welten?

Die fünf Hauptrisiken sind:

Risiken für die Privatsphäre: Die Nutzer geben möglicherweise mehr personenbezogene Daten frei, da die virtuelle Umgebung ein falsches Sicherheitsgefühl vermittelt. Es besteht auch ein Trend zum verhaltensbasierten Marketing durch „Belauschen“ von Avataren.

Avatar-Identitätsdiebstahl und Identitätsbetrug: Diebstahl von Logindaten (Benutzername und Passwort). Hauptmotiv ist die Bereicherung mit echtem Geld, Identitätsbetrug kann aber auch als Mittel zur Rufschädigung eingesetzt werden.

Angriffe auf Handels- und Finanztransaktionen: Rückerstattung von Kreditkartenzahlungen Wenn innerhalb eines Spiels ein Kauf mit einem Online-Bezahldienst (z. B. Kreditkarte oder PayPal) getätigt wird, kann vom Zahlungsdienstleister eine vollständige Rückerstattung gefordert werden (in der Regel innerhalb eines Monats). Erfolgt eine Rückerstattung, ist es technisch und administrativ sehr problematisch, solche Transaktionen rückgängig zu machen.

Risiken für geistiges Eigentum: In virtuellen Welten können mit den vom Dienstanbieter bereitgestellten offiziellen Tools eigene Werke geschaffen werden. Die Rechte der Nutzer sind oft nur vage definiert und können durch verwandte Schutzrechte nichtig werden. Außerdem importieren Nutzer virtueller Welten oft urheberrechtlich geschütztes Material ohne Einwilligung des Rechteinhabers.

Informationssicherheitsrisiken für Minderjährige: Minderjährige können in MMOG (massively multiplayer online games) /virtuellen Welten entweder durch Umgehen der Altersüberprüfungstechniken oder Versagen von Rating-Systemen für Inhalte mit unangemessenen Inhalten konfrontiert werden. Dadurch sind sie Gefahren wie z. B. der Offenlegung realer Kontaktdaten ausgesetzt.

Hinweis: Im Bericht der ENISA sind weitere Risiken aufgeführt.

Wie lauten die wichtigsten Empfehlungen?

Die Empfehlungen betreffen alle von virtuellen Welten betroffenen Gruppen: Wichtige Elemente der Empfehlungen sind Hinweise, wie Nutzer eine Kompromittierung ihrer Daten feststellen können. Dazu kann die folgende Checkliste verwendet werden:

- Ihre Figur ist nicht am selben Ort wie beim letzten Ausloggen.
- Einige ihrer Gegenstände fehlen.
- Ihr Passwort ist falsch.
- Die Liste ihrer Freunde enthält neue Personen.
- Einige Ihrer Figuren fehlen, oder es sind neue Figuren vorhanden.
- In der Kontoverwaltung steht unter „zuletzt eingeloggt“ eine Urzeit, zu der Sie sich nicht eingeloggt haben.
- Sie haben eine E-Mail der Spielleitung (Game Masters) mit einer Warnung in Bezug auf Ereignisse zu einer Zeit, als Sie nicht online waren, erhalten.
- Mitglieder Ihrer „Gilde“ berichten, Ihre Figur zu einer Zeit online gesehen zu haben, als Sie nicht gespielt haben.

Alle Empfehlungen finden Sie in voller Länge im Bericht.

Weitere Informationen finden Sie unter:

http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming

4.8 Sicheres Drucken

Was bedeutet sicheres Drucken?

Unter sicherem Drucken ist jede Maßnahme eines Unternehmens zu verstehen, die gewährleistet, dass Druckgeräte sicher und geschützt bleiben, die Vertraulichkeit, Verfügbarkeit und Integrität der gedruckten oder übertragenen Daten gewahrt bleiben und dass die Organisation bei der Einhaltung einiger Sicherheitsstandards unterstützt wird.

Wie lauten die wichtigsten Empfehlungen?

1. Festlegung eines Dokumenten-Workflows und -Managements
2. Sicherstellung der physischen Sicherheit von Druckgeräten
3. Sicherstellung der logischen Sicherheit von Druckgeräten
4. Gewährleistung der Sicherheit von Druckdaten auf Festplatten oder bei der Weiterleitung an Druckgeräte
5. Prüfung der Flexibilität und Belastbarkeit Ihrer Druckumgebung
6. Verfolgung von gedruckten, kopierten und gescannten Dokumenten zur Weiterleitung als Fax und E-Mail
7. Einrichtung eines Workflows für Berichte über Druckaufträge
8. Festlegung von Unternehmensleitlinien oder -verfahren für die Verwendung von Druckgeräten
9. Organisation von Schulungsmaßmaßnahmen zur Sensibilisierung
10. Festlegung einer Strategie für das sichere Drucken
11. Festlegung von Indikatoren zur Messung des Erfolgs und der Vorzüge der Strategie für das sichere Drucken
12. Festlegung von Ausgangs- bzw. Referenzwerten (Baseline) für die Bewertung
13. Dokumentierung von Lehren und Erfahrungen.

Welche Vorzüge hat sicheres Drucken?

Ein Überblick über die zahlreichen Vorzüge einer sicheren Druckumgebung trägt dazu bei, dass die Organisation (z. B. eine Schule) diesbezüglich fundiertere Entscheidungen trifft. Zu diesen Vorzügen zählen:

- höhere Sicherheit
- höhere Flexibilität durch Lösungen

- geringere Druckkosten (z. B. Ausgaben pro Gerät; Verhältnis zwischen Benutzern und Gerät und Benutzern und Druckvolumen)
- weniger Betrugsfälle
- höhere Mobilität und Flexibilität von Benutzern durch Abkehr vom reinen Kostenstellendenken hin zu einem Ansatz, der das Geschäftspotenzial stärker in den Vordergrund rückt
- bessere Einhaltung von Auflagen und Standards (z. B. Sicherheitsprüfungen auf Basis von Standards wie ISO 27002 oder PCI DSS)
- Durchsetzung von zentralen Kontrollmechanismen für das Netzwerk
- vollständige Verfolgbarkeit von Druckaufträgen
- Flexibilität bei der Rücknahme oder Erteilung von Benutzerrechten
- geringere Anzahl von druckspezifischen Fehler- oder Störungsmeldungen
- Anpassung der Druckumgebung an das Sicherheitsmodell unter Berücksichtigung bewährter Verfahren bezüglich Vertraulichkeit, Integrität und Verfügbarkeit.

Schlussfolgerungen

Auf Druckgeräten werden häufig vertrauliche Informationen wie Rechnungen, Formulare, Mitarbeiterdokumente und Kundendaten be- und verarbeitet. Diese Geräte und die auf ihnen hergestellten Dokumente sind größtenteils nicht geschützt, wodurch Geschäfts- und Transaktionsdokumente anfällig für Sicherheitsverletzungen sind. IT-Manager sollten für sich selbst und ihre Organisation zu einem proaktiven Druckmanagement übergehen, da eine sichere Druckumgebung für jede Organisation ungeachtet ihrer Größe unerlässlich ist. Die Sicherheit der Druck- und Dokumentenumgebung ist ein fester Bestandteil der organisationsinternen und -übergreifenden Sicherheitsstrategie.

Weitere Informationen finden Sie unter:

http://www.enisa.europa.eu/activities/awareness-raising/deliverables/2008/secure-printing-de

5 Schlussfolgerungen und Empfehlungen

Da die Bildung uns alle in unserer Rolle als Schüler oder deren Freunde, Eltern oder Pädagogen betrifft, legt die ENISA den Leserinnen und Lesern nahe, offen für die Sicherheitsinformationen zu bleiben, die sie über alle Informationskanäle erreichen und diese Informationen so viel wie möglich zu nutzen und angemessen zu verbreiten.

Wir empfehlen, die Veröffentlichungen der ENISA zu verfolgen, da sie im nächsten Jahr für den pädagogischen Bereich relevante Sicherheitsprobleme betreffen könnten. Die ENISA wird versuchen, dieses Dokument durch die Aufnahme von Übersichten über neue einschlägige Arbeiten entsprechend zu aktualisieren.

6 Anhang I: Literaturhinweise:

- ENISA Work Programme 2011 for ENISA, the European Network and Information Security Agency(ENISA website) http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011/view (accessed 25 October 2011)
- ENISA and ITU. Guidelines for Parents, Guardians and Educators on Child Online Protection, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative?searchterm=guidelines+for+parents+%2C+guardians (accessed September 2011)
- EUKids Online. Final Report EUKids Online including all findings and recommendations http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf, (accessed 25 September 2011)
- European Commission. 2011 Implementation Report on the Protection of Minors and Human Dignity Recommendations, PROTECTING CHILDREN IN THE DIGITAL WORLD,

  http://ec.europa.eu/avpolicy/reg/minors/rec/2011_report/index_en.htm(accessed September 2011)
- ITU. Measuring the Information Society 2011

  http://www.itu.int/net/pressoffice/press_releases/2011/31.aspx (accessed 16.09.2011)
- The Economist. The great schools revolution, Ed.,17th September 2011,

  http://www.economist.com/node/21529014?fsrc=nlw|edh|09-15-11|editors_highlights (accessed on 17 September 2011)
- Hogben, Giles, Recommendations for Online Social Networks, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks (accessed August 2011)
- Hogben, Giles, Recommendations for Online Social Networks, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks (accessed August 2011)
- Hogben, Giles, Editor, Online Games and Virtual Worlds, European Network and Information Security Agency (ENISA website)

http://www.enisa.europa.eu/act/it/past-work-areas/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming (accessed October 2011)

- Kalmelid, Kjell, Awareness raising quizzes templates: Targeting parents, end-users and SMEs, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/ar/deliverables/2008/ar-quizzes-templates-en, (accessed September 2011)

- Marinos, Louis, Cyber-bullying and online grooming: helping to protect against the risks, European Network and Information Security Agency (ENISA website)

  https://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/Cyber-Bullying%20and%20Online%20Grooming/ (accessed October 2011)

- Santa, Isabella, Children on virtual worlds - What parents should know, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/ar/deliverables/2008/children-on-virtual-worlds (accessed September 2011)

- Santa, Isabella, Secure printing, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/ar/deliverables/2008/secure-printing (accessed October 2011)

- Tirtea, Rodica – ENISA; Castelluccia, Claude – INRIA; Ikonomou, Demosthenes – ENISA, Bittersweet cookies. Some security and privacy considerations, European Network and Information Security Agency (ENISA website)

  http://www.enisa.europa.eu/act/it/library/pp/cookies/?searchterm=cookies, (accessed October 2011)

7 Anhang II: Abkürzungen:

ENISA	Europäische Agentur für Netz- und Informationssicherheit
EU	Europäische Union
ITU	Internationale Fernmeldeunion
AP	Arbeitsprogramm
MS	Mitgliedstaat
NIS	Netz- und Informationssicherheit
SNS	Social-Networking-Internetseiten

8 Anhang III: Verwandte Arbeiten

Organisation		Link
Europarat	Handbuch zur Internet-Kompetenz	http://book.coe.int/EN/ficheouvrage.php?PAGEID=36&lang=EN&produit_aliasid=2023 (Deutsch: http://www.coe.int/t/dghl/StandardSetting/InternetLiteracy/InternetLiteracyHandbook_3_DE.asp)
Eurydice	Schlüsselzahlen zum Einsatz von IKT für Lernen und Innovation an Schulen in Europa 2011	http://eacea.ec.europa.eu/education/eurydice/documents/key_data_series/129DE.pdf

9 Annex IV: Folien für Präsentationen

Folien: Cyber-Mobbing/Online-Grooming:


1 Cyber bullying.pptx

Folien: Kinder in virtuellen Welten:


2 Children on virtual worlds - What parent

Folien: Quiz zur Sensibilisierung:


3 Awareness Raising Quiz Templates.pptx

Folien: Leitlinien für Eltern, Erziehungsberechtigte und Pädagogen:


4 Guidelines for Parents, Guardians ar

Folien: Sicherheitsprobleme bei der Nutzung von Social-Networking-Internetseiten:


5 Security Issues and Recommendatior


6 Cookies.pptx

Folien: Cookies:

Folien: Sicherheitsprobleme in Virtuellen Welten:


7 Virtual worlds-real money.pptx

Folien: Sicheres Drucken:


8 Secure printing.pptx

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu