Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Hintergrund
- Die Risiken
- Kindererziehung

Cyber-Sicherheit für Kinder

Hintergrund

Kindern bieten sich heutzutage unglaublich viele Möglichkeiten auf das Internet zuzugreifen und mit anderen zu interagieren. Neue Dienste im Umfeld der sozialen Medien sprießen wie Unkraut aus dem Boden. Auch viele Anwendungen und Spiele benötigen zwingenden Zugang zum Internet. Außerdem fokussieren sich immer mehr Schulen auf das Internet. Sie nutzen Dienste wie Google Drive, um den Schülern die Möglichkeit zu bieten, Hausaufgaben oder sonstige Schulaufgaben darüber zu erledigen. Kinder wachsen quasi “online” auf. Doch während diese Möglichkeiten eine Menge Vorteile bergen, gehen sie auch mit einigen Risiken einher. Wir werden Ihnen in diesem Newsletter drei Risikofelder aufzeigen, in denen sich Ihre Kinder bewegen könnten, und Ihnen Tipps geben was Sie zu ihrer Sicherheit beitragen können.

Gastautor

Bob Rudis arbeit als Security Data Scientist bei Verizon, ist Autor des Data Breach Investigations Report 2015 und Bändiger von 4 großartigen Kindern. Er hat bei vielen Fortune 100 Unternehmen Programme zur Förderung des Sicherheitsbewusstseins entwickelt und durchgeführt. Sie können ihn auf Twitter als **@hrbrmstr** finden.

Die Risiken

1. **Benehmen**: Wenn Kinder an Online-Gemeinschaften teilnehmen oder in virtuellen Welten unterwegs sind, können sie ein Verhalten an den Tag legen, welches sich von dem in ihrem realen Leben komplett unterscheidet. Das Fehlen der physischen Präsenz kann bei ihnen ein starkes Gefühl von Anonymität erzeugen. Sie sind oft versucht, Verhaltensweisen an den Tag zu legen die andere Kindern verletzen, was man auch als Cyber-Mobbing oder englisch “Griefing” bezeichnet. Ihre Kinder könnten aber auch zum Opfer derartiger absichtlich kränkender Verhaltensweisen von anderen werden.

2. **Kontakt**: Kinder kommunizieren heutzutage fast ständig miteinander, entweder durch Kurznachrichten, in Online-Gemeinschaften, oder beim Spielen in virtuellen Welten. Das Fehlen physischer Präsenz lässt sie schnell vergessen, dass ihr Gegenüber vielleicht nicht derjenige ist, wofür er sich ausgibt oder nicht nur Gutes im Sinn hat. Jäger durchstreifen diese digitalen Welten und werden jede Taktik anwenden, um eine Beziehung zu potentiellen Opfern aufzubauen, oft indem sie sich selbst als Kinder ausgeben.

3. **Inhalt**: Es gibt keinen Mangel an Möglichkeiten, Videos, Tonaufnahmen, Bilder oder textbasierte Nachrichten aufzunehmen und ins Internet zu stellen. Die Versuchung für Kinder, über sich selbst oder andere Familienmitglieder zu viele

Cyber-Sicherheit für Kinder

oder zu private Informationen zu veröffentlichen, ohne dabei die Konsequenzen im echten Leben zu beachten, ist leider beträchtlich. Kindern sind zudem die Gefahren von Identitätsdiebstahl oder der Infektion mit Schadsoftware nicht ausreichend bewusst, wenn andere ihnen trickreich Fragen stellen oder sie zum Klicken auf Links verleiten. Wir leben heute in einer Welt, in der es kein "Rückgängig machen" gibt wenn eine Information einmal im Internet verfügbar ist oder mit anderen geteilt wurde. Kinder halten Posts auf Instagram oder Snapchat vielleicht für flüchtig, aber in Zukunft können diese sie oder andere Familienmitglieder auf vielfältige Weise wieder einholen und zu unerwarteten Konsequenzen führen.

Der Schlüssel zum Schutz von Kindern bei Online-Aktivitäten ist, sie über drohende Gefahren aufzuklären, sich regelmäßig mit ihnen auszutauschen und sie zu motivieren, sich aktiv an ihre Eltern zu wenden.

Kindererziehung

Der beste Weg, Ihre Kinder zu schützen, ist mit ihnen zu reden. Wenn Sie sich darüber bewusst sind, was Ihre Kinder im Internet unternehmen, können Sie sie über die damit verbundenen Risiken aufklären und Ihnen beibringen, wie sie sich schützen können.

1. **Sicherheit zuhause**: Auch in Zeiten großer Mobilität beginnt ein sicheres Online-Verhalten zu Hause. Je früher Sie darüber mit Ihren Kindern sprechen, und Ihre Kinder mit Ihnen, desto besser. Führen Sie regelmäßig Gespräche über Online-Sicherheitsrisiken und berichten Sie dabei über echte, negative Beispiele die stattgefunden haben. Wenn Sie nicht wissen was Ihre Kinder machen, fragen Sie sie einfach. Spielen Sie die ahnungslosen Eltern und bitten Sie sie, Ihnen die neuesten Technologien und wie man sie benutzt zu zeigen. Kinder übernehmen sehr gerne die Lehrer-Rolle und werden sich dabei öffnen. Wenn sie z.B. auf Instagram aktiv sind, bitten Sie sie Ihnen zu zeigen wie Instagram funktioniert, lassen Sie sich einen Account anlegen und diesen Ihren Kindern folgen. Dadurch lernen und überwachen Sie nun nicht nur, was Ihre Kinder machen, es ist auch viel leichter für sie mit Ihnen zu sprechen. Stellen Sie darüber hinaus - so weit das möglich ist - sicher, dass alle Online-Aktivitäten in zentralen Bereichen Ihres Zuhauses stattfinden, und stellen Sie klare zeitliche Nutzungsregeln auf. Wenn Computer zentral aufgestellt sind, werden Kinder viel weniger versucht sein, gefährliche Verhaltensweisen anzunehmen. Stellen Sie eine zentrale Ladestation für Mobilgeräte auf, verbunden mit der Regel, dass alle Geräte dort angesteckt werden, wenn die Kinder schlafen gehen.

2. **Sicherheit außer Haus**: Wenn Kinder nicht zuhause sind, sind sie größeren Risiken ausgesetzt. Helfen Sie ihnen zu verstehen, dass die etablierten Regeln immer gelten. Vermitteln Sie diese Regeln wem auch immer Sie die Betreuung Ihrer Kinder anvertrauen. Wenn Ihre Kinder mobile Geräte haben, überprüfen Sie die Nutzungsmuster

Cyber-Sicherheit für Kinder

(Benutzungszeit, verbrauchtes Datenvolumen) auf Anzeichen einer Umgehung der aufgestellten Regeln. Sie werden nicht alle Übertretungen ahnden können, aber Ihre Kinder werden sich an Ihre besorgten Worte erinnern, wenn sie die Geräte unterwegs nutzen.

3. **Sicherheitsmultiplikatoren**: Sie sind auf dieser Cyber-Patrouille nicht allein und sollten sich mit anderen Eltern, Betreuern, Geschwistern, Lehrern und Freunden zusammenschließen, um die Augen für möglicherweise schädliches Verhalten offen zu halten. Versuchen Sie dafür zu sorgen, dass alle mit den Kindern Schritt halten und aktiv auf die Kinder zugehen, wenn sie sehen, dass diese einen gefährlichen Pfad einschlagen.

Schlussendlich sollten Sie, wenn Kinder einen Fehler machen, jeden einzelnen davon als eine Erfahrung behandeln, aus der man lernen kann, statt ihn direkt mit disziplinarischen Maßnahmen zu ahnden. Erklären Sie immer, warum etwas falsch war, und erinnern Sie sie daran, dass Sie nur versuchen sie vor Gefahren zu schützen, die sie noch nicht sehen (können). Vermitteln Sie ihnen die Sicherheit, sich jederzeit an Sie wenden zu können, wenn sie in eine unbehagliche Situation geraten sind. Achten Sie dabei auch darauf, dass die Kinder auch das Gefühl haben sich an Sie wenden zu können, wenn sie selbst feststellen, dass sie etwas Unangemessenes getan haben. Eine offene, uneingeschränkte Kommunikationskultur ist die beste Art, Kindern in der heutigen digitalen Welt zu helfen, sicher zu sein.

Weiterführende Informationen

Cyber-Mobbing:	http://www.schau-hin.info/extrathemen/cybermobbing.html
Elternratgeber zur Mediennutzung:	http://www.schau-hin.info
Wissen, wie's geht - Wissen rund ums Internet:	http://www.internet-abc.de/eltern/wissen-rund-ums-internet.php
Mehr Sicherheit im Netz:	http://www.klicksafe.de/themen/

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis