

9/2008

www.dud.de

DuD

Datenschutz und Datensicherheit

Recht und Sicherheit in
Informationsverarbeitung
und Kommunikation

Schwerpunkt:
Awareness

Gunter Bitz

Social Engineering

Michael Lardschneider

Mission Security

Heinrich Holst

Privacy im Social Web

Anja Beyer/Gunther Kreuzberger/
Marcel Kirchner/Jens Schmeling

Armin Dewitz, Peter Jürgens

Zu viele Regeln im Sicherheitskonzept?

Weniger ist mehr.

Eine überzeugende Wirkung ist auch in der Kommunikation zum Thema Informationsschutz eine Frage der geeigneten Mittel und der Dosis. Mit zunehmender Komplexität und Menge an Vorschriften und Regeln kann keinesfalls eine höhere Sensibilität und Akzeptanz bei den Mitarbeitern erzielt werden. Ganz im Gegenteil: Ignoranz und – schlimmer – Reaktanz können sich einstellen. Wenige Botschaften, gezielt eingesetzt und humorvoll verpackt haben sich dagegen besser bewährt.

1 Das Regelwerk definieren und verdichten

1.1 Keine Regeln – keine Sicherheit

Regeln begleiten unseren Lebensweg von Kindheit an. Die meisten Regeln sind sinnvoll und nützlich, viele stammen aus unserem Sozial- und Kulturkreis, unserem Rechtsgefüge. Ein Mensch stellt man allerdings berechtigterweise in Frage, zu Neuern fehlen oft noch Regeln. Schließlich leben wir in Zeiten eines dynamischen technischen Umbruchs, von Kriegen ganz zu schweigen.

Regeln leben wir umso mehr, je klarer wir ihren Sinn und Nutzen einsehen. Und

Regeln missachten oder ignorieren wir, wenn wir sie nicht verstehen oder sie uns wertlos erscheinen.

Dies gilt auch für die Regeln zum Schutz von Unternehmensinformationen, Gebote und Verbote, die den richtigen Umgang mit wertvollen Informationen definieren sollen, stehen aktuell in einem besonderen Fokus, weil die Risiken des Verlusts so vielfältig sind. Mitarbeiterinnen und Mitarbeiter müssen neue Regeln ohne großen Zusatzaufwand erfassen und blind verstehen. Die Vorschriften sollten im Alltag praktikabel anwendbar sein und dürfen den Arbeitstag nicht behindern. Niemand soll ständig darüber nachdenken müssen, ob er sich in jedem Moment seines Handelns konform zu den Regeln der Informationssicherheit verhält. Denn letztlich will jeder von uns so flexibel, effizient und effektiv wie möglich arbeiten können.

Bestimmend ist, wer die absolut notwendigen Regeln zu publizieren – und zwar so klar, dass sie im Alltag problemlos anwendbar sind.

1.2 Regelwerke neigen dazu, ein verstaubtes Dasein zu fristen

Regeln werden von Sicherheitsfachleuten formuliert und nicht von Texten. Deshalb sind sie oft kompliziert und wenig alltagstauglich. Holen Sie deshalb Ihre Regeln aus den Regelwerken heraus. Für die Umsetzung in die Kommunikation gilt dann zunächst eine einfache Checkliste:

- Hinterfragen Sie noch einmal Sinn und Nutzen jeder einzelnen Vorschrift.

Abb. 1 |



- Beurteilen Sie realistisch, was wäre, wenn es eine Vorschrift nicht gäbe.
- Verzichten Sie mutig auf Überflüssiges.
- Formulieren Sie die wichtigsten Regeln verständlich und praxistauglich.
- Geben Sie Tipps und bieten Sie Lösungen an.
- Zeigen Sie in konkreten Alltagssituationen auf, wie man sich vorbildlich verhält und wie nicht.

1.3 Der richtige Umgang mit sensiblen Unternehmensinformationen

Verantwortliche in Ihren Unternehmen müssen sich konsequent um die Einsetzung der Schutzverantwortung der Information kümmern – jede Führungskraft für den eigenen Verantwortungsbereich und jeder Projektleiter bereits zum Projektstart. Dabei ist unerheblich, in welcher Form die Information vorliegt oder ent-



Armin Dewitz

ist Geschäftsführer der Dewitz, Selzer, Partner Werbeagentur GmbH, spezialisiert auf Awareness-Konzepte für Informationsschutz.

E-Mail: armin.dewitz@dewitz-selzer-partner.de



Peter Jürgens

der Initiator von Walt & Friends, kümmert sich seit vielen Jahren um die Sensibilisierung für ein angemessenes Verhalten im Umgang mit schutzwürdigen Informationen.

E-Mail: pj@privatjgma.de

Abb. 2



stelt. Legen Sie eindeutige Kriterien für die Klassifizierung der Schutzwürdigkeit fest. Machen Sie eine Risikobewertung, welcher wirtschaftliche Schaden Ihre Imageschaden sind. Wenn Unternehmen stattdessen ermitteln, wenn Informationen in falsche Hände geraten?

Achten Sie darauf, dass das Volumen an streng vertraulichen Informationen im Vergleich zu dem der vertraulichen und dem der übrigen internen Informationen angemessen ist.

Legen Sie bei der Definition und regelmäßigen Überprüfung Ihrer Verhaltensvorgaben den Fokus auf die wirklich schutzwürdigen Informationen. Unterscheiden Sie hier zwischen Vertraulichem und Streng Vertraulichem.

Qualifizieren Sie Ihre Mitarbeiterinnen und Mitarbeiter nicht mit zusätzlichen Regeln für den Umgang mit beruflichen, internen Informationen. Sichtlich sind auch diese internen, aber eben nicht besonders sensiblen Informationen wertvoll. Dennoch gilt es vorrangig, das besonders Wertvolle, eben das Vertrauliche und streng Vertrauliche, zu schützen.

Die Umsetzung „streng vertraulich“ sollte ausschließlich von dem Personalkreis vergeben werden, der das Risiko des Missbrauchs dieser besonders sensiblen Informationen wirklich realistisch einschätzen und bewerten kann. Es bietet sich daher an, dass nur der Vorstand bzw. die Geschäftsführung eines Unternehmens sowie die für die Bereiche Recht und Risikomanagement verantwortlichen Führungskräfte den Status „streng vertraulich“ vergeben. So halten Sie das Volumen überschaubar und bleiben als Unternehmen im Praxisalltag uneingeschränkt arbeitsfähig.

Selbstverständlich geben Sie auch für den Umgang mit streng Vertraulichem

entsprechend angemessene Verhaltensvorgaben. Kommunizieren Sie über diese besonderen Vorschriften konsequent nur an die, die tatsächlich mit diesen höchst sensiblen Informationen umzugehen haben. Betonen demnach damit keine Mitarbeiterinnen und Mitarbeiter, die nicht mit streng Vertraulichem in Berührung kommen.

Konzentrieren Sie sich bei der Definition aller weiteren Verhaltensregeln auf den Schutz vertraulicher Informationen. Auch hier gilt die Devise „Weniger ist mehr.“ Achten Sie auf Angemessenheit und Praktikabilität.

Vermitteln Sie anschließend die Regeltexte nur im Hintergrund Wort für Wort. Erläutern Sie lieber, was die Regel für die tägliche Praxis sagen will, und wie ihr Einhalten den Schutz der Unternehmensinformationen verbessert.

Geben Sie zu jeder Regel konkrete Verhaltensbeispiele aus der täglichen Praxis. Wählen Sie dabei auch unbewusst fehlerhafte Geschehnisse vor Augen. Thematisieren und visualisieren Sie sensibelverständliche mögliche Gefahren.

1.4 Beispiele zum allgemeinen Verhalten im Umgang mit Vertraulichem

Zeigen Sie Ihren Mitarbeiterinnen und Mitarbeitern auf, dass Schweigen in der Öffentlichkeit Gold ist.

Machen Sie Bekanntes bewusst, beispielsweise, dass im Arbeitsumfeld wie auch dahinter das Konzept „Keine Geheimnisse – Keine Diebstahl“ Wirkung zeigt.

Jedem wird einleuchten, dass das Wegschließen von vertraulichen Dokumenten und Mobilien (Notebook, Speicherstick, BlackBerry etc.) sowie das Verschlusseln der Daten auf Mobilien vor Diebstahl sowie vor unberechtigtem Zugriff schützt – egal ob im Büro, unterwegs oder dabei.

Motivieren Sie dafür, dass der Einsatz seiner persönlichen Kennwörter schützt. Sie geben keines etwas an und dürfen nicht zu ernten sein.

Speichern Sie Empfehlungen aus, wie man Vertraulich bei per Post oder per E-Mail sicher versendet, was es beim Kopieren oder Faxen von Vertraulichem zu beachten gilt.

Erläutern Sie, warum und wie man vertrauliche Dokumente sorgsam vernichtet oder Dateien mit vertraulichem Inhalt nicht wiederherstellbar macht.

Abb. 3



Inkarnieren Sie, wie man einem defekten PC oder nicht mehr benötigten Datenträger (DVD, CD etc.) entsorgt.

Mit bewährten Empfehlungen für ein angemessenes Verhalten sorgen Sie dafür, dass Regeln automatisch angewendet und eingehalten werden, ohne sie im exakten Wortlaut zu kennen.

1.5 Organisatorische Voraussetzungen schaffen

Definieren Sie keine Regeln, bevor Sie nicht organisatorisch dafür gesorgt haben, dass Sie im Alltag umgesetzt werden können.

Stellen Sie einheitliche Vorlagen in elektronischer Form (z.B. für Word, PowerPoint) bereit, damit die Kennzeichnung eines Dokuments als vertraulich oder streng vertraulich bereits während der Erstellung am PC vorgenommen werden kann.

Unterstützen Sie organisatorisch und technisch die Vergabe persönlicher, gebotener „starker“ Kennwörter. Geben Sie gegebenenfalls Tipps, wie man eine Vielzahl unterschiedlicher Kennwörter vergibt und sich diese merken kann, ohne sie „öffentlich“ aufschreiben zu müssen.

Wenn Sie ein Wegschließen fördern, so können Sie sich frühzeitig darum, dass der Schranckschlüssel existiert und funktioniert bzw. eventuell gar ein Tresor vorhanden ist.

Schreiben Sie verschlüsselte Speicherung auf Mobilien vor, so haben Sie selbstverständlich vorab die entsprechende Installation in der Festplattenverschlüsselung vorzunehmen. Stellen Sie verschlüsselte Speichersticks zur Verfügung.

Auch eine verschlüsselte E-Mail-Kommunikation entsteht nicht von selbst. Unterschätzen Sie den Aufwand hierfür nicht!

Abb. 4



Klämmern Sie sich am Schredder und Aktenstapler nicht erst dann, wenn sich Nachfragen oder Beschwerden häufen. Undrogen-Soda für, das DVD's und CDs ordnungsgemäß entsorgt werden können.

1.6 Sicherheit im Job und zuhause

Die Erfahrung zeigt deutlich, dass Tipps und Hilfen fürs Private sehr gefragt und andersherum wertvolle Wirkung im Unternehmen nach sich ziehen. Ihre Umsetzung bewirkt nicht nur ein sicherheitsbewusstes Verhalten des Einzelnen dabei, Sie führt indirekt zu einem bewussten Umgang mit sensiblen Informationen am Arbeitsplatz und unterwegs.

Bieten Sie zum Beispiel von Sicherheitssoftware (Virenscanner, Firewall...) auf privaten Computern.

Speichern Sie Empfehlungen für Software zur Verschlüsselung der privaten Festplatten (Desktop, Notebook, externe Festplatten) und Speichersticks aus. Empfehlen Sie sichere, verschlüsselte Speichersticks.

Bieten Sie Mitarbeiterinnen und Mitarbeitern des Service, private vertrauliche Dokumente im Büro zu schreddern und DVDs oder CDs und ggf. alte PCs über Ihren IT-Dienstleister sicher zu entsorgen.

Wenn Sie die neue dargestellte Erfahrungen und Empfehlungen aufgreifen, werden Sie sicherlich einen großen Schritt bei der Sensibilisierung Ihrer Mitarbeiterinnen und Mitarbeiter machen.

Jetzt kommt es noch auf die Verpackung an. Auch hierzu gibt es ein mehrfach bewährtes Konzept.

2. Das Kommunikationskonzept

2.1 Kontrast: je komplexer die Aufgabe, desto einfacher der Stil

Wenn wir einerseits die realistischen Risiken zur Kommunikationssicherheit abbilden wollen und andererseits die Handlungen nicht herpetisch oder sogar als Risikofänger bebildern und beifließen wollen, liegt die Abstraktion über einem Comic eigentlich schon auf der Hand.

Wir zeigen zum Beispiel mit Walt & Friends, welche Kommunikationsfreiheiten wir gewissen Walt & Friends ist eine fiktive Abteilung, der man bei der Arbeit zuschauen kann. Alle Handlungsspielarten sind möglich und erlaubt, natürlich nur bis zu einer vom Unternehmen zugelassenen Grenze. Die Scheu im Kopf gibt es dennoch nicht, wenn auf Seiten des Auftraggebers akzeptiert wurde, dass es sich um eine satirische Überhöhung der Inhalte und nicht um seine Gage handelt.

Jeder kann sich so in Walt, Penny, Polynese, Fran, Sheldon und Jess spiegeln. Das muss nicht immer passen – niemand ist genau so, aber jeder kennt irgendwo genau so einen Kollegen. Jedenfalls hat jeder schon einmal solche zum Teil recht bizarren Szenen im beruflichen Umfeld erlebt oder sie erlebt bekommen. Wenn wir ehrlich sind, erkennen wir uns und unsere Mitmenschen in ihrer Nicht-Perfektion wieder. Walt & Friends ist genauso liberal! Und das macht den Charme dieser Comicfiguren aus.

Einzigartige Humortransportieren wichtige Inhalte.

Dieser Humor ist deshalb glaubwürdig, weil die Botschaften nicht behärdend oder infantil daher kommen, sondern auf sympathische Art zwischen sind. Entscheidend ist auch, dass wir mit Walt & Friends eine insgesamt lockere, hilfsbereite und lösungsorientierte Abteilung angezogen haben. Niemand in hier kriminell oder anstrengend verhalten. Es sind die kleinen Schwächen im Verhalten, die Fehler oder

Abb. 5 | Animation für Intranet-TV oder Bildschirmtext.



Abb. 6



© by Dinklage, Steiner, Pöcher - Heiß, Dinklage

auch nur die Ratslosigkeit, vor einer Herausforderung zu stehen, für die man noch keine oder erstmal eine mackewürdige Lösung hat. Vor dieser Situation stehen wir doch täglich. Alles ist im Wandel, immer gibt es Neues und oft ist korrektes Verhalten mit komplexen Prozessen verknüpft.

Jetzt kommen wir zum zweiten Mehrwert dieses Konzepts. Unser Ansatz zur Informationssicherheit problematisiert nicht, er bietet Handlungs- und Lösungsvorschläge. Gut, die gibt es auch im Handbuch. Dort sind sie aber schon so beschreiben, dass sie zu Alltagskonflikten passen – von der Komplexität der Texte meist ganz zu schweigen. Comics dienen uns als kommunikative Trojaner, um mit unseren einfachen Handlungsvorschlägen in die Köpfe der Zielgruppe zu kommen. Kurz – wir machen aus der Not eine Tugend. Das Thema Informationsschutz ist nicht gerade beliebt – wir schreiben aus der Langeweile hoch, indem wir das Problem grafisch angehen, überzeichnen – um dann erneut zu erkennen, dass die Charaktere das ja gar nicht böse gemeint haben. Zum Glück gibt es dann ja auch noch eine Lösung – Anhalten – alles halb so schlimm. Dieser Kontrast macht das Konzept aus.

Abb. 7: Comics wurden auch in WIP-Anwendungen integriert



2.2 Eine Entwicklung nach einem klaren Masterplan?

Wlat & Friends ist schon mehrere Jahre bei verschiedenen Unternehmen auch in adaptierten Form und in individueller Ausprägung im Einsatz. Schön, wenn das, was heute besteht, alles nach einem ausgefeilten Plan realisiert worden wäre. Nein, die ersten Vorschläge entstanden gut gelegen an einem Stichtisch im Büsselerker Flughafen. Die ersten Skizzen waren da noch richtig, die Dialoge etwas sperrig, die Verhaltensstipps zu lang, meist noch zu sehr am Text der Security Policy orientiert. Heute gibt es über 150 Cartoons, noch mehr Einzelzettel und viele Animationen, die die Kernkernern zum Informationsschutz sehr locker integrieren. Und die Verhaltensstipps haben sich in Zusammenarbeit mit den Kunden immer deutlicher an der täglichen Arbeitspraxis orientiert und wurden damit auch immer kürzer. Nebenbei bemerkt, haben sich auch die Cartoons im Laufe der Jahre gelockert und haben mehr Profil gewonnen.

2.3 Wie entstehen die Ideen?

Jedenfalls nicht mehr allein durch den Blick in die Security Policy. Wir lassen uns von den Gesprächen mit den Fachleuten inspirieren, die uns wesentlich mehr Input geben als eine durch alle Bänder gegossene schriftliche Plattform. Nicht dass die verabschiedete Sicherheitsrichtlinie nicht wichtig ist. Sie ist der unvermeidliche Kodex, die Rechtschauer des Handelns im Unternehmen und gibt uns damit auch das inhaltliche Gerüst. Aber wenn uns belächelt werden wird, dass die Mitarbeiter schon morgens im Bus zur Arbeit eilen und lautstark über vertrauliche Dinge diskutieren, ist dies ein schnell zu lösendes Problem aus dem Alltag. Und schon wieder die Idee für einen neuen Cartoon mit der entsprechenden Botschaft.

Das Thema erfindet sich täglich neu. Daher sind kurze Reaktionszeiten entscheidend. Wir können ein Thema mit einem Cartoon sehr schnell umsetzen. Ein neues Foto, ein Film oder eine Veranstaltung sind da wesentlich langsamer, immer teurer und oft zu spät realisierte Alternativen. Insgesamt lassen wir uns lieber von dem kleinen Umständlichkeiten, den peinlichen Geschichten oder auch oft unmissbaren Vorfällen anregen, um daraus eine neue Story zu entwickeln, die dann natürlich zur Security Policy passen muss. Manches übersteht die Entwurfsphase nicht, obwohl der Gag gut war. Aber es geht ja nicht um Humor zum Selbstzweck, sondern um die Vermittlung von Inhalten. Und so ganz leicht lässt sich der Humor auch nicht aus dem Ärmel schütteln, es handelt sich hier schließlich nicht um Stand-up-Comedy, sondern um ein Edukationskonzept zur Änderung des Verhaltens von erwachsenen Menschen.

Abb. 8 |



2.4 Wir müssen die Zeitkosten unserer Zielgruppe füllen, nicht leeren

In immer weniger Menschen haben die Zeit, sich mit Regelthesen an ihren Kernaufgaben zu beschäftigen. Unternehmensstrukturen verschärfen, die Verantwortung liegt zunehmend auf der handhabenden Ebene, relevante Informationen müssen in kurzer Zeit selektiert und bewertet werden. Zur Auseinandersetzung mit einer textlastigen, stark verschlüsselten Awareness-Botschaft fehlt ganz einfach die Aufmerksamkeit. Die Wenigsten lesen gerne lange Texte. Auch eine umfängliche schriftliche Security Policy wird diesen Anreiz nicht bieten.

Wir sollten uns darüber im Klaren sein, dass manche Regeln auch stören und nerven, manche sind nicht praktikabel, was sich erst später herausstellt, vieles ist hier oder dort gar nicht relevant, was der Autor gar nicht so wusste. Es gilt also, Ballast abzuwerfen. Oder neudeutsch: den Informations-Overflow in den Griff zu bekommen.

2.5 Einen Cartoon und einen kurzen Tipp schafft jeder

Wir müssen die Informationen verdichten und die Regelwerke für die individuelle tägliche Praxis "übersetzen". Das ist aber noch nicht genug. Nicht alle Regeln sind für alle von Bedeutung.

Wer über die normale nicht öffentliche Arbeit hinaus ebenfalls mit vertraulichen Unterlagen in Kontakt kommt, muss nicht unbedingt über den Umgang mit streng Vertraulichem informiert werden. Wer keinen BlackBerry verwendet, muss den Umgang mit ihm nicht lernen und wer keine Dienststreifen macht, muss die Vorschriften für die Sicherheit auf Reisen

nicht im Detail kennen. Hier gilt es, die Botschaft zu selektieren und für die intenzionierten Zielgruppen zu bündeln.

Auf dieser Basis werden Übungsvorschläge formuliert, die zu einer Kenntnis der Risiken und zu einer Schärfung der Aufmerksamkeit bei der Zielgruppe führen sollen – im Idealfall zu einer Verhaltensänderung.

Als Verstärker dienen dann zusätzliche Hinweise auf den privaten Einsatz oder den konkurrenz Vorteil als Add-on. Beispiel: Das Angebot, vertrauliche private Daten auf CD oder DVD auch in der Firma zu entsorgen, oder die Verschlüsselungsvorschläge auch für die Home-Anwendungen zu nutzen.

3 Fazit

Die höchste Sicherheit bietet nicht die sorgfältige Security Policy im Handbuch, sondern das richtige individuelle Verhalten

Abb. 9 |

