known_sense
_identity _kreation _kommunikation _knowledge
VIRUSQUARTETTDE

TOOLS & SERVICES
FÜR SECURITY-MANAGEMENT & -PROMOTION
SECURITY-NEWSLETTER 02 FEB.2005

Awareness ist Psychologie

Warum sich Mitarbeiter selbst ENTsichern – Qualitative Studie deckt die geheime Logik der IT/Information Security in Unternehmen auf

Erfahrungsgemäß ist die Wirksamkeit der bisher üblichen didaktischen Methoden bzw. Awareness-Maßnahmen im Bereich der IT/Information Security begrenzt. Irgendetwas hält viele Mitarbeiter davon ab, die ihnen weitgehend bekannten Sicherheitsmaßnahmen auch in die Tat umzusetzen. Die Tatsache, dass z.B. Schulungen u.a. Trainingsveranstaltungen an Grenzen stoßen, ohne dass diese Grenzen offensichtlich werden, lässt darauf schließen, dass die Probleme, die durch unachtsame Mitarbeiter entstehen, entweder unbewusst sind oder im Rahmen von didaktischen Settings nicht offen bzw. ungenau oder nicht in ihrer umfänglichen Drastik angesprochen werden.

Auf diese und ähnliche Störstellen und Barrieren werden wir bei known_sense sehr häufig angesprochen. Als Security-Dienstleister, dessen Tools und Services im Bereich Awareness bewusst auf das know-how einer erfahrenen Kommunikationsagentur setzen, erwarten unsere Kunden Antworten auf diese und weitere Fragen zum Thema Awareness, die weder mithilfe herkömmlichen BWL-Lateins noch mit der üblicher Management-Methoden genügend beantwortet werden können.

Zahlreiche Unternehmer und Security-Officer, denen wir unsere Konzepte vorstellen, gehen inzwischen soweit, zu fragen, warum sich Mitarbeiter oder Kollegen - in der Regel überdurchschnittlich begabte und besonnene Menschen - quasi selbst aktiv ENTsichern, auch dann, wenn umfangreiches Security-Wissen bzw. regelmäßig intensive Schulungsmaßnahmen diese ENTsicherungen eigentlich verhindern sollten.

„Vergesslichkeit", sagen die einen. „Faulheit" die anderen. Wir bei known_sense vermuten: Hinter dem, was der Einfachheit halber unter derlei Schlagwörtern und weiteren (austauschbaren) wie etwa „Unkonzentriertheit" oder gar „Sabotage" subsummiert wird, stecken in Wahrheit Verhaltensprinzipien, die nach einer bestimmten „geheimen" Logik funktionieren. Wenn diese offensichtlich verdeckten Prinzipien untersucht und verstanden werden würden, könnte jedes Unternehmen auch seine Mitarbeiter und deren Verhalten in punkto Sicherheit besser verstehen und sein Personal effizienter einstellen.

Um aber diese Mitarbeiter-Verfassungen und die damit verbundenen Wirkprinzipien zu enkodieren, mithin tatsächlich sichtbar werden zu lassen, müssten im Rahmen von Awareness kulturelle Rahmenbedingungen ausgelotet und der Fokus stärker auf Kommunikation und Psychologie gesetzt werden als auf Richtlinien, Kontrolle oder technologische Details, die in der Regel die „eigentlichen" Motive verdecken sollen. ➔

Die Themen

>> **Awareness ist Psychologie** Warum sich Mitarbeiter selbst ENTsichern - Qualitative Studie deckt die geheime Logik der IT/Information Security in Unternehmen auf

>> **Von Innen nach Außen und umgekehrt** – Zwei Einsatzszenarien für Securitygames: Teil II

>> **Neues Security-Brettspiel „Firewall":** Viren gegen „Mauersteine"

Impressum

Herausgeber:
Dietmar Pokoyski
known_sense
Kaiser-Wilhelm-Ring 30-32
D-50674 Köln
Fon +49 221 91277778
securitytools@known-sense.de
www.virusquartett.de
www.known-sense.de

➔ Wie stark Unternehmenskultur mit Information Security verknüpft ist und welche Rolle die Psychologie dabei spielt, lässt sich anhand von Beispielen beschreiben, die hypothetisch mögliche Wirkprinzipien verdeutlichen sollen.

1. Security ad absurdum

Stellen Sie sich vor, ihr ganzes Leben lang wäre Ihnen gesagt worden – und zwar von Ihren Eltern, Tanten und Onkels, von ihren Lehrern, ihren Freunden und sogar von Ihrem Chef und Ihrem Bundestagsabgeordneten –, Sie müssten nur gut in der Schule sein, einen ordentlichen Beruf lernen und Ihren Vorgesetzten folgen um dann nach einem (1!) Job und knapp 40 Jahren Arbeit auf dem Buckel mit 65 eine hübsche Rente zu erhalten. Pustekuchen, wie wir alle wissen. Ähnlich – nur mit umgekehrten Vorzeichen – ergeht es denjenigen, die (noch) über Arbeit verfügen dürfen. Diese sehen sich aktuell über Medien, Unternehmen, deren Interessensverbände und einer zunehmend in wirtschaftlichem Pragmatismus verstrickten Politik mit dem Leitsatz konfrontiert: „Du musst MEHR Risiko eingehen!"

Passwort als Brühwürfel für Wünsche: Ein Bild sagt mehr als 1.000 Worte. Und in einem Passwort wollen sich viele Bilder unterbringen lassen.

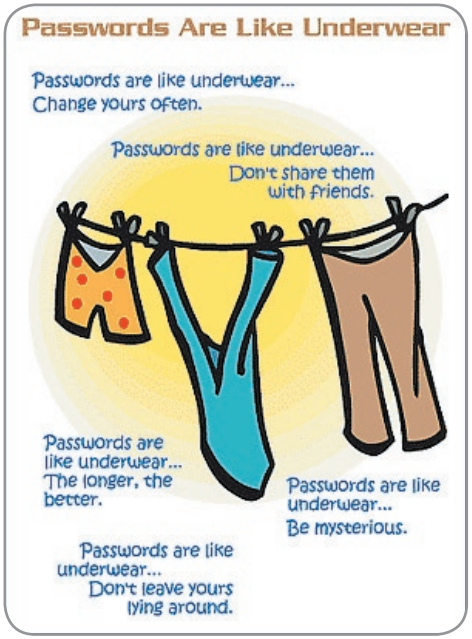
Ein Unternehmen, das Mitarbeiter entlässt, sie mithin ENTsichert und von den Verbliebenen die Aufweichung ihrer Arbeitsplatz-Versicherung fordert, gleichzeitig aber Ihre Information Security in einem hohen Maße kultiviert, kann das Geld für Security Awareness im Grunde direkt aus dem Fenster werfen, wenn es diesen, von den Mitarbeitern zumindest unbewusst wahrgenommenen Widerspruch „Risiko versus Security-Kultur" nicht offensiv durch geeignete begleitende kommunikative Maßnahmen auflöst.

2. Nicht ohne digitalem Nippes

Mehr Risiko bedeutet aber auch mehr Selbstverantwortung und ergibt eine engere Verzahnung von Privatleben und Arbeit. Der Lebensraum wird Arbeitsraum und umgekehrt, die Arbeitsstätte (wenn sie es nicht schon war) zum Lebensmittelpunkt, eine Situation, die u.U. auch mit einer zunehmenden Anonymisierung einhergeht. Was für alle Freiberufler seit jeher Realität darstellt, steht den meisten Angestellten, etwa in Form der sehr trefflich bezeichneten „Ich-AG" noch bevor.

So deuten unsere psychologisch ausgebildeten Berater und Coaches dann auch Passwörter als „Brühwürfel für Wünsche". Denn laut einschlägiger Studien, wählen Mitarbeiter an IT-Arbeitsplätzen als Log-in überwiegend sinnvolle Begriffe und damit „schlechte", sprich triviale Passwörter, die noch dazu in der Regel positive Assoziationen vermitteln, z.B. Namen von Partnern, Kindern oder Freunden oder Begriffe, die mit den Begriffsfeldern Urlaub/Reise/Freizeit und Co. verknüpft sind (Man beachte in diesem Zusammenhang auch einmal die Nähe der Bezeichnung „Passwort" zu „Passport" = Ausweis!). Wenn nun Passwörter quasi als Medium genutzt werden, um Beziehungen zu stärken oder Emotionen eine Basis zu verleihen, so sagt das sehr viel über die Unternehmenskultur der hiesigen Companies und die (mögliche) Bindungslosigkeit Ihrer Mitarbeiter.

Bereits seit langem ist aus der Kulturpsychologie über Lebensräume (resp. Arbeitsräume) bekannt, dass der Mensch das Bedürfnis verspürt, seinen Mittelpunkt mehr oder weniger individuell auszugestalten. Kaum ein Büro, in dem nicht auch Fotos der Liebsten Schreibtische zieren oder Aufkleber, Poster,



„Brühwürfel" für Führungskräfte? In jedem Fall mehr Wunsch als Wirklichkeit und mit der in IT-Kampagnen oft üblichen Portion „Schlüpfrigkeit": Passwörter werden im Claim einer bekannten wie populistischen Kampagne mit Unterwäsche asssoziiert.

persönliche Kaffeetassen mit eigenem Namenszug ein „Besetzt" proklamieren. „Dies ist der Platz von Hans Schmidt. Hier arbeite ich, habe Erfolge, freue mich und leide. Ich bin Fan von Schalke 04. Und das auf dem Foto ist meine Familie." So oder so ähnlich lauten in der Regel die Botschaften personalisierter Arbeitsplätze.

Was das alles mit Information Security zu tun hat? Ein wie oben beschriebener Gestal-➔

➔tungsdrang hat bereits seit langem auch den digitalen Raum vollständig erfasst: Statt PE oder Baryt in Rahmen sind es nun Bitmaps auf dem Desktop. Gadgets oder private Favoriten im Browser und Mails von und an Freunden. Störstellen, die Security-Verantwortlichen die Haare zu Berge stehen lassen, weil sie für Infrastruktur der IT im Unternehmen ein erhebliches Risiko darstellen. „Digitaler Nippes", behaupten die meisten Administratoren (und sind dabei meist selber die „schlimmsten Dekorateure").

Unternehmen, die allerdings eine private Ausgestaltung und Nutzung von IT-Arbeitsplätzen untersagen, fördern bei Ihren Mitarbeitern, durch das bloße Verbot der Arbeitsplatzgestaltung ein seelisches Vakuum, das dann durch Verlagerung auf andere Szenarien wieder belebt und bewegt werden will, z.B. durch sinnige und somit triviale Passwörter (s.o.) oder eine Verlebendigung, die sich Sicherheitslücken zunutze macht.

3. Mein Security-Leck. Mein Hacker. Mein „Freund".

Denn gerade dort, wo der mechanische, IT-gestützte Umgang dem zu Routine erstarten (Arbeits-)Leben auch den letzten Fun-ken an Thrill nimmt, sind z.B. Malware und Cybercrime eine willkommene Abwechslung, die Mitarbeitern zu (Ersatz-) Spannung verhilft, wenn eine solche durch Arbeit bzw. individualisiertes Arbeitsumfeld nicht gewährleistet ist. Unterm Strich ist z.B. die „Einladung" an einen Hacker, etwa über eine aktive ENTsicherung eines Mitarbeiters, eine äußerst erfolgsversprechende Strategie, Beziehungen zu schaffen.

Grundsätzlich ist anzunehmen: Je mehr Security-Policies die Individualität am Arbeitsplatz einschränken, je restriktiver diese gehandhabt werden, umso größer der Wunsch des Einzelnen nach weiterem Spielraum und umso spannender die Wahrnehmung von Sicherheitslücken und das Austesten ihrer Folgen – eine Dynamik, die bestimmten Persönlichkeiten offensichtlich einen regelrechten Kick versetzen kann.

Fazit: Unternehmen, die im Falle von Stellenabbau selber ENTsicherung betreiben, die individuelle Ausgestaltung und private Nutzung von IT-Arbeitsplätzen restriktiv behandeln oder über Unternehmenskultur oder den falschen Einsatz von Technologie Anonymisierung fördern, sollten geplante Awareness-Massnahmen zum Thema Security als integrierte Kommunikationskampagne ausrichten, mögliche Widersprüche in ihrer Unternehmenskultur offensiv und transparent anpacken und täten darüber hinaus gut daran, bindungslosen Mitarbeitern Alternativen zur Entfaltung ihrer Persönlichkeit anzubieten ■

„ENTsicherung am Arbeitsplatz – Die geheime Logik der IT/Information Security in Unternehmen"

Um die hier beschriebenen und andere Beobachtungen zu verifizieren und weitere psychologische Faktoren auszuloten, die der Optimierung von Awarenessmaßnahmen dienen, wird known_sense im Sommer 2006 und in Kooperation mit psychologischen Marktforschern eine Studie unter dem Arbeitstitel „ENTsicherung am Arbeitsplatz – Die geheime Logik der IT/Information Security in Unternehmen" produzieren. Die Untersuchung hat zum Ziel, die ‚eigentlichen', wahrscheinlich z. T. unaussprechbaren Aspekte zu ergründen, die im Umgang mit dem Thema IT/Information Security eine Rolle spielen.

Hierfür werden 15 Personen, darunter Mitarbeiter aller Unternehmensebenen, auch Entscheider und Security-Officer, in 2-stündigen Interviews von speziell ausgebildeten Interviewern nach Ihrer Haltung, ihren Erfahrungen, ihren Erwartungen und Wünschen in punkto IT-Security befragt.

In tiefenpsychologischen Interviews können die verdeckten Motive, die grundsätzlich das Verhalten im Umgang mit Information Security beeinflussen, erfasst und in einen Sinnzusammenhang gebracht werden, aus dem ihre Handlungsrelevanz verständlich wird.

Erfahrene Psychologen decken hierbei in knapp zweistündigen Einzelexplorationen die unbewussten seelischen Wirkungen und Einflussfaktoren auf, die das Security-Verhalten der Mitarbeiter bestimmen. Unsere Probanden werden aktiviert, in ihrer eignen Sprache zu erzählen, was ihnen zum Thema „Security" einfällt. So werden die Interviews zu einer gemeinsamen Forschungsreise von Proband und Interviewer. Dabei werden alle verborgenen, nicht bewusst wahrgenommenen Bedeutungskontexte, seelische Motive und Einflussfaktoren erschlossen und offen gelegt, so dass sich am Ende neue Perspektiven mit vielleicht überraschenden Wendungen ergeben.

Auf Basis dieser repräsentativen Ergebnisse können dann zielgenaue und konkrete Empfehlungen zu innerbetrieblichen Maßnahmen hinsichtlich der Verbesserung von Security formuliert und z.B. bessere Awarenesskampagnen konzipiert werden. ■

Von Außen nach Innen und umgekehrt - Zwei Einsatzszenarien für Securitygames (Teil II)

Zwei Beispiele unterschiedlicher Ansätze für den Einsatz des Virusquartetts (www.virusquartett.de) als Kommunikationstool demonstrieren die vielfältigen Verwendungsmöglichkeiten von Spielen im Bereich der Security-Promotion bzw. -Awareness.

Nachdem im ersten Teil der Nutzen des Kartenspiels für die externe Kommunikation in Form von Messe-Promotion unseres Agenturkunden GiT beschrieben wurde, geht es im folgenden um die Optimierung der internen Kommunikation eines Finanzdienstleisters und eben um das Schlagwort Security-Awareness.

Unser Kunde, der ungenannt bleiben möchte, wurde Anfang 2005 aufgrund der zahlreichen positiven Medienberichte über das Virusquartett auf uns aufmerksam. Er stand kurz vor der Einführung einer sehr umfangreichen Security-Policie. Die Implementierung sollte, um Aufmerksamkeit und Akzeptanz bei den Mitarbeiten (Anzahl im unteren vierstelligen Bereich) zu erzielen, durch eine Plakatkampagne begleitet werden. Die Realisation dieser Kampagne wurde über die Köpfe der für die Security-Policie verantwortlichen IT-Abteilung hinweg durch das unternehmensinterne Marketing an die Hausagentur delegiert.

Kurz vor dem geplanten Launch konnten die IT-Verantwortlichen die Unternehmensführung von der mangelnden Kompatibilität der Kampagnen mit ihren ursprünglichen Zielen überzeugen. Diese würde in ihrer Intention ganz offen mit allzu moralischen Bildern arbeiten, die zu sehr auf Droh- bzw. Bestrafungsszenarien (im Falle der Nichteinhaltung der Policie) setzen.So wurden die 8 Entwürfe, an denen mehr als ein halbes Jahr gearbeitet wurde, eingestampft.

Die Aufgabe:
Erste Hilfe auf Low-Budget-Basis

Als Ersatz wurde known_sense ins kalte Kampagnen-Wasser geworfen. Nach dem Briefing ging es uns in etwa so, wie man es z.Z. von der gesamten deutschen Ärzteschaft vernehmen kann: Man kommt mit einer Tasche voller neuer, schöner und scharfer Skalpelle in eine Ambulanz mit nahezu unheilbaren Patienten, die dazu über keinerlei Kassenbonität verfügen. Denn die ziemlich schnörkellos gestellte Aufgabe lautete in etwa: „Entweder ihr gestaltet uns innerhalb von nicht ganz vier Wochen eine kommunikative Begleitung der Policie-Implementierung, z.B. auf Basis des bereits vorhanden Kartenspiels, oder wir geben die Unterlagen ganz ohne Rahmenkampagne aus." Oder anders: Wie erzeugt man angesichts der knappen Zeitressourcen eine sinnvolle Belebung der Mitarbeiter-Kommunikation? Eine Belebung, die zu einem konstruktiven Feedback an die Policie-Produzenten führt? Eine, die auch speziell diesen hilft, das Security-Management dynamisch weiter zu entwickeln? Das alles zu einem Etat, der aufgrund der bereits verworfenen Kampagne auf knapp 20% der ursprünglichen Summe eingedampft war.

Step 1:
Basis erspüren und Propaganda-Felder aussäen

Was war also zu tun? Wir konnten und mussten nicht lange über Konzepte nachdenken und „mischten" uns nach und zwischen den Briefings zunächst 2 halbe Tage lang unter die Mitarbeiterschaft, loteten deren Arbeitsräume aus, beobachteten die Menschen en passant bei ihren Jobs und ihrer Kommunikation und unterhielten uns auf einer zunächst ganz unverbindlichen Ebene mit Ihnen, z.B. in der Mensa oder während der Kaffee- und Zigarettenpausen. Anschließend luden wir sie kurzfristig und ganz offiziell zu Workshops ein und erarbeiten nach einem Warm-up, bei dem u.a. auch das Virusquartett erstmals vorgestellt wurde, gemeinsam mit ihnen auf Basis der Policie erste Entwürfe für Leitsätze zur Security-Kultur des Unternehmens. Denn die Policie beschrieb sehr ausführlich, wer was wie und wann zu tun oder zu lassen hat – man hatte allerdings vergessen, die essentiellen Inhalte auf Kernsätze zu fokussieren, die auch außerhalb der IT-Abteilung verstanden und umgesetzt werden konnten, die memorierbar sind und sich darüber hinaus auch innerhalb verschiedener Medien einer begleitenden Kampagne als Claims bzw. Slogans eigneten.

Dietmar Pokoyski (known_sense): „Man kommt mit einer Tasche voller neuer, schöner und scharfer Skalpelle in eine Ambulanz mit nahezu unheilbaren Patienten, die dazu über keinerlei Kassenbonität verfügen. "

Step 2:
Visuelle Brücken schaffen Aufmerksamkeit

Die durch die IT-verantwortlichen und Unternehmensführung bearbeiteten Leitsätze publizierten wir gemeinsam mit Verweisen auf die ausführlichere Darstellung in der Policie im Rahmen eines kleinformatigen, aber auffällig gestalteten Leporellos, der in der Verpackung des Virusquartetts an jeden Mitarbeiter ausgegeben wurde. Hierbei kam uns der enge Zeitrahmen sehr entgegen, denn die jeweiligen Abnahmen durch die Entscheider wurden ungewohnt kurzfristig erledigt.

Während synchron hierzu die Policie über das Intranet publiziert wurde, suchten wir als Vertriebsort für das Spiel mit Leporello eine Location aus, die jeder Mitarbeiter wenigstens einmal pro Woche aufsucht: Die unternehmenseigene Mensa, in der unser Tool gemeinsam mit Essensmarken ausgegeben wurde. Hier erhielten Spiel und Leitsätze eine wesentlich höhere Aufmerksamkeit als bei einem Vertrieb über Auslage an den jeweiligen Arbeitsplätzen. Denn dort hätte sich das Produkt der Konkurrenz aktueller Jobprojekte oder stets verfügbarer Medien wie Inter- und Intranet erwehren müssen.

Als visuelle Reminder wurden darüber hinaus Auszüge aus den Leitsätzen als so genannte „Security-Tags" auf den gebrandeten Kartenrückseiten des Virusquartetts und in der Woche des Launchs auch auf Essensmarken und Mensa-Tischsets gedruckt. Die typographisch markanten und visuell durchaus attraktiven Tags waren unverwechselbar mit den Leitsätzen und der Implementierung der Policie verknüpft und erhielten so einen gewissen →

➔Logo-Charakter. Wir druckten die Tags auch auf einem Laserdrucker auf A-4-Seiten aus, die wir innerhalb des Unternehmens verteilten, indem wir sie an schwarze Bretter hefteten oder an belebten Locations kommentarlos mit Tesafilm an Wände und Türen klebten. So wurde eine Brücke zwischen den Arbeitsräumen, dem Spiel und der damit verknüpften Policie geschaffen, die auf die (wenn auch unbewusste Wahrnehmung) der neuen Sicherheitsstandards abzielte - eine Maßnahme, die angesichts des geringen Etats eine kostengünstige, aber durchaus effiziente Alternative zu einer neuen, wahrscheinlich auch weitaus aufwendigeren Plakatkampagne darstellte.

Nachdem das Spiel von nahezu allen Mitarbeitern äußerst positiv aufgenommen worden war, implementierten wir eine Online-Variante innerhalb des Intranets. Die Sieger der Online-Trumpfspiele wurden geranked. Die Motivation, zu spielen und (in möglichst kurzer Zeit) zu gewinnen wurde durch die Unternehmensleitung noch forciert, indem für Wochen- und Monatsbeste spontan attraktive Incentives ausgelobt wurden. Und auch im Intranet fungierten die bereits eingeführten Security-Tags als Reminder, quasi in Form assoziativer Illustration (in Sinne einer rein visuellen Duftmarke) ohne tatsächlichen inhaltlichen Kontext in Bezug auf die einzelnen Text-Beiträge.

Step 3:
Integration des Unternehmensumfelds

Dass Security-Kultur eines Unternehmens auch außerhalb der räumlichen Basis wirkt, wissen vor allem diejenigen, die intensiv auf Mitarbeiter mit mobilem Equipment setzen. Mitarbeiter, die ihre mobilen Geräte auch zuhause oder unterwegs in Hotels bzw. bei Kunden nutzen. Security kann eben nicht wie ein Ausweis oder Schlüssel beim Verlassen der Firma an Werkspforten abgegeben werden. Und so, wie mobile Geräte aus den Unternehmen um den Globus geschickt werden, verbreitete sich auch das Virusquartett bei Familien, Freunden, Kunden oder Geschäftspartnern unseres Kunden und erweckte Neugier. Aus diesem Grund wurde in Step 3 auf ausdrücklichen Wunsch der Mitarbeiterschaft eine 2. Auflage des Kartenspiels produziert, aus der jeder Mitarbeiter eine Hand voll Spiele an sein privates wie geschäftliches Umfeld abgeben konnte - wohlgemerkt nicht als klassisches Giveaway mit hohem Streufaktor und entsprechendem Werbewert, aber immerhin (quantitativ) mit einer ausreichenden Quote und (qualitativ) mit sichtbarer Leidenschaft, die auch das Umfeld spüren ließ, dass das Unternehmen Security-Kultur nun intensiver lebte als zuvor.

So wurde aus einem Instrument, das zunächst ausschließlich für den internen Einsatz vorgesehen war, Schritt für Schritt ein (wenn auch limitiertes) Promotionstool, eine Dynamik, über die - exakt umgekehrt - bereits im ersten Teil dieser Story berichtet wurde.

Da known_sense diese Awareness-Maßnahme bisher lediglich als Kreationsinkubator begleitet hat, können wir an dieser Stelle keine verbindliche Auskunft über einen möglichen messbaren Erfolg abgeben. Dass man bei unserem Kunden durchaus von einem Erfolg ausgeht, beweist die aktuelle Anfrage, die Kampagne in Kürze fortzusetzen - diesmal glücklicherweise nicht als Notaufnahme, sondern in Form einer Prophylaxe mit dem beruhigenden Wissen um die (relative) Gesundheit des Patienten. ■

Den ersten Teil können Sie in unserem ersten Newsletter nachlesen oder unter (http://www.securitymanager.de/magazin/artikel_835_von_aussen_nach_innen_und_umgekehrt_-_zwei.html).

Neues Security-Brettspiel „Firewall"

Bei jedem Angriff werden bisher verdeckte Stärken für einen kurzen Moment offenbart. Man gewinnt wichtige Informationen über die Aufstellung des Gegners. Der ist entweder ein Virus oder Teil einer strategischen Abwehrmaßnahme: die Firewall.

„Firewall" ist ein kurzweiliges Brett- oder Computerspiel für 2 bzw. 1 Person(en) und eignet sich für jeden, der sich auf spielerische Weise mit dem spannenden Thema „Firewall" (bzw. verwandte IT-Security-Themen) auseinandersetzen will.

Bei „Firewall" sind Mittel und Ziele quasi asymmetrisch: der Angreifer versucht mit seinen 6 Virensteinen die Firewall zu durchdringen, der Verteidiger versucht dies mit seinen 6 Firewall-Steinen zu verhindern. Die Spielsteine haben unterschiedliche Stärken (1, 2, 3). Gezogen wird auf einem Spielbrett, das durch die (bedruckte) Innenseite einer äußerst promotionfreundlichen Würfelverpackung gebildet wird. Es besteht aus 36 Feldern, aufgeteilt in 3 Zonen (rot, grün, blau). Besondere Spannung entsteht dadurch, dass man als Spieler nur die Stärke der eigenen Steine sieht, während die gegnerischen verdeckt sind.

Viren- gegen Mauersteine

Die Virensteine versuchen, die grüne Zone zu erreichen. Die Firewallsteine versuchen, das zu verhindern.

Das Spiel ist für die Viren gewonnen, wenn sie 3 Steine in die grüne Zone gebracht haben. Das Spiel ist für die Firewall gewonnen, wenn klar ist, dass die Viren das nicht mehr schaffen können. Mut, Cleverness und ein gutes Gedächtnis entscheiden bei „Firewall" über Sieg oder Niederlage.

Branding ab 500 Promo-Games

Der Spielaufbau ist handlungsorientiert, so dass verschiedene Spielsituationen in „Firewall" Realszenarien aus der IT-Security entsprechen.

„Firewall" kann ab einer Auflage von 500 Exemplaren, individualisiert gebrandet, produziert werden. ■

Im nächsten Newsletter stellen wir Ihnen eines unserer zahlreichen Tools zum Thema Passwortschutz vor: "Hack mich" ist ein Kartenspiel für 2-8 Personen, von denen derjenige gewinnt, der als erster die Passwörter seiner Gegner herausfindet.