

**Securing Your
Digital Life**

Risikogesteuerte Authentifizierung: Immer das richtige Maß an Sicherheit und Bequemlichkeit

Endverbraucher, die das Internet täglich nutzen, verlangen personalisierte Angebote und erwarten, dass ihnen nahezu alle Angebote online zur Verfügung stehen. Für die Anbieter bedeutet dies, jedem Kunden eine Online-Identität einzurichten, die kontinuierlich verwaltet und vor allem gesichert werden muss.

Gleichzeitig nehmen Identitätsbetrug, die verbrecherische Übernahme von Benutzerkonten und andere Angriffe auf digitale Identitäten und Transaktionen zu. Diese Attacken schüren Verbraucherängste und untergraben das Vertrauen in Online-Dienste. Erste Angebote verzeichnen bereits nachlassende Benutzerzahlen.

Dieses Whitepaper stellt ein Produkt vor, das zur Abwehr der beschriebenen Gefahren jedem Risiko mit dem richtigen Maß an Sicherheit begegnet – je nach Anwender, Transaktion und Applikation. Die Entrust-IdentityGuard-Plattform bietet starke, risikoabhängige Authentifizierungstechnik. Sie sichert den Zugriff auf Onlinedienste bei geringen Kosten und geringstmöglichem Einfluss auf die Benutzerfreundlichkeit auch bei hohen Benutzerzahlen.

8. November 2005

Entrust ist eine eingetragene Marke von Entrust, Inc. in den Vereinigten Staaten und in einigen anderen Ländern. Entrust ist eine eingetragene Marke von Entrust Limited in Kanada. Alle anderen Firmen- und Produktnamen sind Marken bzw. eingetragene Marken ihrer jeweiligen Eigentümer. Die Angaben in diesem Dokument dienen nur zu Informationszwecken und sind nicht als Empfehlung zu verstehen. Bevor Sie auf der Grundlage dieser Informationen Handlungen vornehmen oder unterlassen, sollten Sie zunächst einen Fachmann konsultieren. ENTRUST ÜBERNIMMT KEINE GEWÄHR FÜR DIE QUALITÄT, RICHTIGKEIT ODER VOLLSTÄNDIGKEIT DER IN DIESEM ARTIKEL ENTHALTENEN INFORMATIONEN. SOLCHE INFORMATIONEN WERDEN WERDEN OHNE MÄNGELGEWÄHR BEREITGESTELLT, UND ENTRUST ÜBERNIMMT KEINERLEI ZUSICHERUNGEN UND/ODER GEWÄHRLEISTUNGEN, WEDER EXPLIZITE NOCH IMPLIZITE, GESETZLICH ODER DURCH HANDELSBRAUCH ODER ANDERWEITIG BEGRÜNDETE GEWÄHRLEISTUNGEN UND LEHNT SÄMTLICHE ZUSICHERUNGEN UND/ODER GEWÄHRLEISTUNGEN DER MARKTGÄNGIGKEIT, DER ZUFRIEDEN STELLENDEN QUALITÄT, DER NICHTVERLETZUNG VON SCHUTZRECHTEN ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUSDRÜCKLICH AB.

INHALTSVERZEICHNIS

EINFÜHRUNG	1
ONLINE-IDENTITÄTEN IN GEFAHR	1
IDENTITÄTSBETRUG NIMMT RAPIDE ZU.....	1
ONLINE-DIENSTE ERLEIDEN VERTRAUENSVERLUST	2
DER GEFAHR BEGEGNEN	2
REGULIERER FORDERN STARKE AUTHENTIFIZIERUNG	3
EVALUATIONSKRITERIEN FÜR STARKE GEGENSEITIGE AUTHENTIFIZIERUNG.....	3
ENTRUST IDENTITYGUARD 8.0 – EINE FLEXIBLE AUTHENTIFIZIERUNGSPLATTFORM	4
ANWENDERAUTHENTIFIZIERUNG	4
WECHSELSEITIGE AUTHENTIFIZIERUNG	7
RISIKOGESTEUERTE SICHERHEIT	8
FLEXIBLE RICHTLINIENGESTALTUNG	8
AKZEPTANZ DURCH BENUTZERFREUNDLICHKEIT	9
EINFACHE UND KOSTENGÜNSTIGE EINFÜHRUNG	9
PREISWERTE AUTHENTIFIZIERUNGSMITTEL	10
INTEGRATION OHNE TIEFE SYSTEMEINGRIFFE	10
MEHRKANAL-AUTHENTIFIZIERUNG	11
ARCHITEKTUR UND INTEGRATION	11
INTEGRATION MIT GERINGEM AUFWAND	11
ROBUSTE, FLEXIBLE ARCHITEKTUR.....	11
ZUSAMMENFASSUNG	12
WEITERFÜHRENDE TEXTE	12

Einführung

Angriffe auf Online-Identitäten nehmen rapide zu. Typische Beispiele sind Phishing-Attacken und der Einsatz von Malware zu Spionagezwecken. Von Januar bis August 2005 wuchs beispielsweise die Anzahl der Phishing-Sites, die die Basis für viele der genannten Attacken darstellen, um über 200 Prozent.¹ Alarmierend ist, dass der Diebstahl von Identitätsdaten immer häufiger tatsächlich gelingt.

Das Risiko, das aus diesen Angriffen erwächst, liegt nicht allein in direkten finanziellen Verlusten. Als viel problematischer erweist sich der Einbruch des Vertrauens bei den Verbrauchern. Er stellt das Einsparpotenzial in Frage, das sich Unternehmen davon erhoffen, übers Telefon oder in Filialen abgewickelte Transaktionen auf das Internet zu verlagern.

Von Oktober 2004 bis Oktober 2005 haben bereits 18 Prozent der Nutzer von Online-Banking-Diensten aus Furcht vor Angriffen auf ihre persönlichen Identitätsdaten ihre Online-Transaktionen entweder verringert oder sogar ganz eingestellt.²

Angesichts der Bedrohungslage leiten staatliche Institutionen in vielen Ländern Maßnahmen ein, die die schnellere Implementierung zusätzlicher Sicherheitsmechanismen vorantreiben. Ein Beispiel für entsprechende Initiativen ist die Richtlinie der US-amerikanischen Federal Deposit Insurance Corporation (FDIC), einer Institution, die die Liquidität von Banken sichert. Die FDIC fordert stärkere Authentifizierung für Onlinedienste von Finanzdienstleistern bereits für 2006.³

Schritte zum Schutz der digitalen Identitäten seiner Kunden gehören in dieser Situation für jedes Unternehmen zum aktuellen Pflichtprogramm, wenn es seine Internet-Dienstleistungen ausbauen und davon wirklich profitieren will. Dieses Whitepaper untersucht die damit verbundenen Aufgaben und stellt neue Werkzeuge vor, die den Kampf gegen den Identitätsbetrug gewinnen helfen.

Online-Identitäten in Gefahr

Den Kern von sicheren Online-Transaktionen bildet die zweifelsfreie Erkennung des Anwenders durch den Dienst und des Dienstes durch den Anwender. Die Kunden müssen im sicheren Gefühl arbeiten können, tatsächlich mit dem von ihnen gewünschten Service der richtigen Organisation verbunden zu sein und nicht mit einer gefälschten Site. Der Dienstleister wiederum muss wissen, dass ein legitimer Benutzer und kein Betrüger mit ihm in Verbindung tritt.

¹ Anti-Phishing Working Group, August 2005, Activity Report

² Entrust Online Banking Survey, Oktober 2005

³ FDIC Financial Institution Letter FIL-103-2005, 12. Oktober 2005

Kennwörter allein reichen heute nicht mehr aus, um auf beiden Seiten das notwendige Maß an Sicherheit herzustellen.

Identitätsbetrug nimmt rapide zu

Identitätsbezogene Online-Attacken wie die unberechtigte Übernahme von Benutzerkonten gehören zu jenen Delikten der Kriminalstatistik, die sich am schnellsten ausbreiten. Die Gartner Group hat ermittelt, dass von Mai 2004 bis Mai 2005 weltweit cirka 1,2 Millionen Kunden zusammen etwa 929 Millionen US-Dollar allein durch Phishing-Attacken verloren haben.⁴ Gleichzeitig erleiden auch Anbieter signifikante Verluste. Einige Online-Banken und andere Dienstleister etwa kommen ganz oder zum Teil für den Schaden auf, den ihre Kunden durch Online-Identitätsbetrug erleiden.



Die Kompromittierung der Online-Identität eines Anwenders kann dem Angreifer den Zugriff auf dessen Online-Konten und den Zugang zu weiteren persönlichen Informationen ermöglichen. Diese Form des Identitätsbetrugs ist deshalb so beunruhigend, weil sich der Angreifer weder in der Nähe seines Opfers aufhalten muss noch physischen Zugang zu irgendwelchen Dokumenten benötigt. Die einzige Herausforderung für den Dieb ist es, das Opfer zur Herausgabe seiner Kennwörter zu bewegen – danach stehen ihm die gleichen Funktionen offen wie einem legitimen Benutzer.

Wer weiter auf Kennwörter setzt, leistet dem Online-Betrug Vorschub. Phishing-Angriffe locken Anwender mit gefälschten E-Mails auf ebenfalls gefälschte Websites, die dazu benutzt werden, Kennwörter, PINs und TANs zu stehlen. Diese Angriffe funktionieren deshalb so gut, weil die Angreifer das wohlbekannte Erscheinungsbild der Webseiten und E-Mails von Banken, Online-Shops und Kreditkarten-Anbietern bis ins Detail nachahmen.

⁴ Gartner Security Survey, 23. Juni 2005

Die betrügerischen E-Mails kommen oft vorgeblich vom Support der vertrauten Online-Anbieter. Sie verlangen unter einem Vorwand, dass der Anwender seine User-Daten preisgibt – einige Mails behaupten sogar, dies sei für eine Sicherheitsüberprüfung oder ein Update der Security-Maßnahmen notwendig. Mit diesen Daten gelangen die Betrüger dann an die Benutzerkonten der Anwender.

Bei Malware-Attacken installieren die Angreifer heimlich Spionagesoftware auf dem Computer des Opfers. Entweder verleiten E-Mails oder betrügerische Angebote auf Webseiten den Anwender zum Download der Malware, oder die Angreifer schicken die Programme direkt als E-Mail-Attachments oder schleusen sie über bekannte Schwachstellen in verbreitete Anwendersoftware oder Betriebssysteme ein. Eine typische Form der Spionagesoftware sind beispielsweise „Keylogger“, die Tastenanschläge und Mausbewegungen inklusive eingetippter Kennwörter aufzeichnen und die Daten an den Angreifer weiterleiten. Mit noch ausgefeilteren Angriffsmethoden gelingt es sogar, während einer noch laufenden Online-Sitzung des Anwenders betrügerische Transaktionen durchzuführen. Diese neue Angriffsform verbreitet sich deutlich schneller als traditionelle Phishing-Attacken – so hat die Zahl der Websites, die entsprechende Malware beherbergen, von Mai bis August 2005 um über 360 Prozent zugenommen.⁵

All diese Attacken können nur dort gelingen, wo Ein-Faktor-Authentifizierung per Kennwort im Einsatz ist. Nur unter dieser Bedingung nämlich steht dem Angreifer, der in den Besitz von User-Name und Kennwort gelangt ist, bereits das gesamte Online-Konto seines Opfers für eine größere Zahl von Operationen zur Verfügung. Für die Attraktivität und damit die Zunahme dieser Attacken ist darüber hinaus entscheidend, dass die Angreifer übers Internet problemlos und kostengünstig eine große Zahl von Angriffsversuchen zugleich starten können: Die Betrüger kommen bereits auf ihre Kosten, wenn nur ein kleiner Teil ihrer Attacken Erfolg hat.

Online-Dienste erleiden Vertrauensverlust

Attacken auf die Online-Identität erschüttern das Vertrauen der Konsumenten und die Akzeptanz von Online-Geschäften. Den bereits erwähnten 18 Prozent der Anwender von Online-Banking-Diensten, die aus Angst vor Identitätsdiebstahl Angebote seltener oder gar nicht mehr wahrnehmen⁶, stehen ähnliche Akzeptanzprobleme bei Online-Shops gegenüber. Hier haben 48 Prozent der Teilnehmer einer Umfrage angegeben, dass sie Käufe im Internet vermeiden, weil sie befürchten, dass ihre Finanzdaten gestohlen werden könnten.⁷

⁵ [Anti-Phishing Working Group, August 2005 Activity Report.](#)

⁶ [Entrust Security Survey](#), April 2005.

⁷ [Computer Security Industry Association.](#)

Die Kunden werden bei ihrer Zurückhaltung bleiben, wenn sie nicht sehen, dass etwas für die Sicherheit ihrer Online-Identitätsdaten getan wird. Die Anbieter sehen sich deshalb mit zwei negativen Auswirkungen der Identitätsdiebstähle konfrontiert:

1. Zunehmende direkte Kosten, die aus der Regulierung von erfolgreichen Angriffen entstehen und
2. spärliche Nutzerzahlen, aufgrund derer die Dienste nur noch Kosten generieren und keinen Ertrag mehr erwirtschaften.

Gleichzeitig genießen Unternehmen, die das Problem aktiv angehen und ihren Kunden bessere Schutzmaßnahmen anbieten, signifikante Vorteile. Eine Untersuchung von Entrust hat ergeben, dass 68 Prozent der Konsumenten, die als Internet-Nutzer noch nicht Online-Banking betreiben, dies in Betracht ziehen würden, wenn ihre Online-Identität besser geschützt sei.⁸ Sogar bei Kunden, die bereits auf Online-Banking-Angebote zugreifen, gäbe es einen positiven Effekt: 90 Prozent gaben an, sie würden auch höherwertige Dienste nutzen, wenn sie ihre Identität besser geschützt sähen.

Der Gefahr begegnen

In drei Schlüsselbereichen sollten Anbieter dem Identitätsbetrug entgegenreten:

- **Erkennung:** Das Monitoring der Internet-Umgebung hilft, Angriffe auf Online-Identitäten schnell zu erkennen. Typischerweise bedeutet dies, mit Filtern und Anomalie-Detektoren nach Mustern von Phishing-Mails und Malware-Attacken zu suchen, um im Falle eines Angriffs unverzüglich einschreiten und den Schaden begrenzen zu können.
- **Reaktion:** Sobald ein Angriff erkannt wurde, muss die betrügerische Website, die die Anwender-Identitäten abfängt, so schnell wie möglich vom Netz genommen werden. Dies erfordert im Normalfall die Zusammenarbeit mit den ISPs. Außerdem ist es sinnvoll, schnellstmöglich Warnungen auf den eigenen Seiten zu publizieren.
- **Schadenseingrenzung:** Die Auswirkungen eines Angriffs einzugrenzen, wenn dieser bereits stattfindet, ist eine der wichtigsten Maßnahmen zur Eindämmung von finanziellen Verlusten und zum Erhalt des Anwendervertrauens. Die Implementierung entsprechender Prozeduren stellt für die meisten Organisationen allerdings eine besonders große Herausforderung dar.

Maßgebliche Institutionen empfehlen außerdem übereinstimmend, starker gegenseitiger Authentifizierung Priorität einzuräumen.

⁸ [Entrust Internet Security Survey](#), September 2004.

Regulierer fordern starke Authentifizierung

Der Wirtschaftszweig der Online-Services genießt bei internationalen Regulierungsinstanzen hohe Aufmerksamkeit. Sie reagieren auf Bedrohungen sofort. In den USA etwa rät die Federal Deposit Insurance Corporation (FDIC) ausdrücklich dazu, für die Kunden ein Upgrade von existierender Ein-Faktor-Authentifizierung per Kennwort auf Systeme mit Zwei-Faktor-Authentifizierung durchzuführen.⁹ Zuletzt publizierte die FDIC eine Forderung, stärkere Authentifizierung für Transaktionen mit hohem Risiko bereits bis Ende 2006 einzuführen.¹⁰ Auch das Financial Services Technology Consortium hat reagiert. Es empfiehlt Unternehmen der Finanzbranche ausdrücklich, bessere gegenseitige Authentifizierungsprozeduren zu prüfen und zu implementieren.¹¹

In Europa will EU-Binnenmarktkommissar Charlie McCreevy die Bankkunden im Falle von Phishing-Betrug besser stellen. Ein Richtlinienentwurf, der Ende November 2005 der Süddeutschen Zeitung vorlag, weitet die Rechte der Verbraucher aus und will die Banken verpflichten, Zahlungen aus manipulierten Überweisungen generell zu ersetzen.¹² Damit verlagert sich das Risiko des Identitätsbetrugs im Internet in höherem Maße auf die Anbieter, die dem Problem deshalb mit besserer Authentifizierungstechnik entgegenwirken sollten.

Gegenseitige Authentifizierung ist deshalb ausdrücklich Teil vieler Empfehlungen, weil sie es dem Anwender zusätzlich zum Schutz der Anmeldedaten gegen Diebstahl erleichtert, gefälschte Webseiten zu erkennen. So ist er auch gegen immer neue Angriffsformen besser gewappnet.

Evaluationskriterien für starke gegenseitige Authentifizierung

Starke gegenseitige Authentifizierung ist eine wirkungsvolle Maßnahme gegen verschiedene Formen des Identitätsdiebstahls. In einer Umgebung mit Millionen von Kunden allerdings spielt nicht nur der Sicherheitsgewinn eine Rolle, sondern auch die Bedienbarkeit. Wenn Authentifizierungstechniken mit zu hohem Aufwand für Endanwender verbunden sind, suchen die User nach Umgehungsmöglichkeiten. Online Dienste, die mit allzu lästigen Prozeduren geschützt sind, lassen sie sich ganz verleiden. Zu teure Systeme schließlich können sich viele Online-Anbieter gar nicht erst leisten.

Aus diesen Überlegungen ergeben sich folgende Evaluationskriterien für Authentifizierungslösungen:

- **Hohe Sicherheit.** Heute gängige Kennwort-Anmeldesysteme sind schwach. Zu ihrer Überwindung reicht es, die Kennwörter des Anwenders zu stehlen oder die eingetippten Anmeldedaten abzufangen. Außerdem geben die Systeme dem Anwender selbst keine Sicherheit, dass er überhaupt mit der richtigen Anwendung oder Website verbunden ist. Authentifizierungssysteme müssen deshalb Mechanismen bereitstellen, mit denen die Benutzer die Authentizität der aufgerufenen Site überprüfen können. Sie müssen außerdem einen zweiten Authentifizierungsfaktor neben dem Kennwort bieten, um die Online-Identität des Anwenders besser zu schützen.
- **Flexibel und Risikogestützt.** Authentifizierung wird immer häufiger mit einer Ermittlung des jeweiligen Zugriffs- und Transaktionsrisikos verbunden und dem jeweiligen Risiko dynamisch angepasst. Wenn ein Bankkunden etwa seinen Kontostand von zuhause aus prüft, besteht ein geringeres Risiko, als wenn er von einem unbekanntem Terminal aus eine internationale Überweisung veranlasst. Zugleich akzeptiert der Kunde bei Transaktionen von geringem Wert keine aufwändigen und unbequemen Anmelde- und FreigabeprozEDUREN. Online-Organisationen müssen deshalb in der Lage sein, verschiedene Authentifizierungsmethoden anzubieten.
- **Anwenderfreundlichkeit.** Akzeptanz ist für alle Sicherheitslösungen ein kritischer Erfolgsfaktor. Wenn ein bestimmter Ansatz zu beschwerlich oder verwirrend ausfällt, wenden sich vor allem Konsumenten schnell wieder ab und suchen entweder nach Alternativen zum Online-Angebot oder wechseln sogar den Anbieter. In beiden Fällen zahlt sich die implementierte Sicherheitslösung nicht aus.
- **Einfache und kostengünstige Einführung.** Viele Sicherheitslösungen wurden für den internen Bedarf von Unternehmen und deren Mitarbeitern entwickelt. Auf die Implementierung und den Betrieb in extrem großen Umgebungen mit einer heterogenen Benutzerbasis sind sie nicht ausgelegt, und sie generieren unter solchen Einsatzbedingungen zu hohe Einführungskosten. Brauchbare Lösungen für derartige Umgebungen müssen preiswert sein und sich vorhandenen Infrastrukturen leicht anpassen lassen.

Berücksichtigt eine Authentifizierungslösung diese Punkte nicht, besteht immer die Gefahr, dass sie entweder zu unsicher ausfällt oder das Ziel verfehlt, das Vertrauen der Anwender in die Online-Dienste zurückzugewinnen.

⁹ [Putting an End to Account-Hijacking Identity Theft](#), FDIC, 14 December 2004.

¹⁰ [FDIC Financial Institution Letter FIL-103-2005](#), October 12, 2005.

¹¹ [FSTC Counter-Phishing Initiative](#), December 2004.

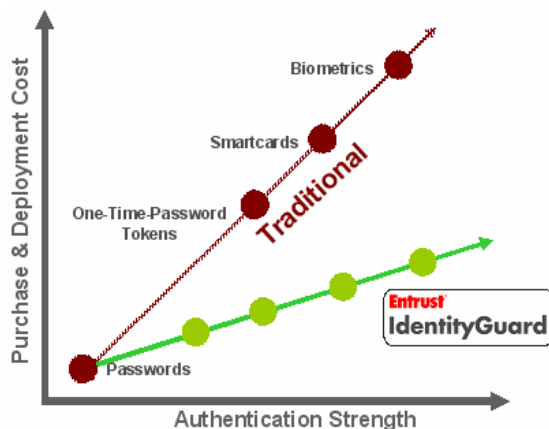
¹² Meldung auf www.a-i3.org vom 27. November 2005

Entrust IdentityGuard 8.0 – eine flexible Authentifizierungsplattform

Entrust IdentityGuard 8.0 ist eine wechselseitig arbeitende Authentifizierungsplattform, die dem aktuellen Bedarf von Online-Organisationen gerecht wird. Mit dem Ziel der Flexibilität entwickelt, erlaubt sie eine maßgeschneiderte Anpassung der Authentifizierungsprozeduren an das jeweils festgestellte Risikoprofil und an die Präferenzen der Anwender. Jede Authentifizierungsmethode der Lösung wurde auf besondere Benutzerfreundlichkeit hin ausgelegt und kann zu einem Bruchteil der Kosten angeboten werden, die Systeme mit zeitsynchronen Hardware-Tokens verursachen.

Anwenderauthentifizierung

Gegen Identitätsbetrug lässt sich mit einem zweiten, getrennten Faktor zur Anwendererkennung vorgehen. Dabei handelt es sich oft um einen Gegenstand, den der Anwender besitzen und griffbereit halten muss, wenn er sich anmeldet – neben dem Kennwort, dass er wissen muss. Diese Technik verhindert, dass der Anwender seine gesamte Online-Identität beispielsweise an eine betrügerische Website verliert, die in den Besitz seiner Kennwörter gelangt. Ohne den physischen Anmeldefaktor nämlich gewinnt der Angreifer keine Gewalt über das Konto des Opfers.



Bei Entrust IdentityGuard behalten die Anwender bereits vorhandene Anmeldenamen und Kennwörter auch nach der Implementierung des Systems. Die Anmeldung wird allerdings durch weitere Authentifizierungsfaktoren ergänzt und deshalb sicherer. Damit sich das System sowohl den Vorlieben der Anwender als auch dem Ergebnis der jeweiligen Risikobewertung anpassen kann, arbeitet es mit einer reichen

Auswahl unterschiedlicher Authentifizierungstechniken. Keine davon erfordert es, den Anwender mit zusätzlicher Hard- oder Software auszustatten. Die verwendeten Methoden entsprechen außerdem denen, die die amerikanische FDIC-Studie „Putting an End to Account-Hijacking Identity Theft“ aufführt, die sich mit Maßnahmen gegen Identitätsdiebstahl befasst.¹³

- *Nicht Hardware-gestützte Einmalkennwort-Karte* oder „Grid-Authentifizierung“,
- *Shared Secret* („gemeinsames Geheimnis“ oder „wissensgestützte Authentifizierung“),
- *Geräteauthentifizierung* und
- *Out-of-Band-Authentifizierung* (Authentifizierung über getrennten Kanal).

Grid-Authentifizierung. Bei der Grid-Authentifizierung steht dem Anwender als zweiter Anmeldefaktor während seiner Online-Aktivitäten eine Tabelle zur Verfügung, deren Zeilen und Spalten per Zufallsprinzip erzeugte, individuell verteilte Zeichen und Ziffern enthalten. Solch eine Tabelle lässt sich auf eine separate Karte oder etwa auf eine vorhandene Kredit- oder Bankkarte drucken. Das „US Patent and Trade Office“ hat das Grid-Authentifizierungsverfahren als Patent anerkannt. Wie die Grid-Karten jeweils konkret aussehen, entscheidet der Betreiber des Systems. Die Zelleninhalte der Tabelle können numerisch oder alphanumerisch ausfallen oder aus beliebigen Zeichenkombinationen bestehen – je nach Anforderung der Anwendung, die damit geschützt werden soll. Auch die Größe der Tabelle lässt sich anpassen.

Praktisch läuft die Authentifizierung per Grid-Karte folgendermaßen ab: Der Anwender gibt zunächst seinen Anmeldenamen und sein Kennwort ein, wie er es gewohnt ist. Danach schaltet sich die Grid-Authentifizierung ein und fragt den Anwender, welchen Inhalt seine Grid-Karte in bestimmten Tabellenzellen zeigt. Indem er die Fragen richtig beantwortet, weist er nach, dass er sich im Besitz der ihm zugeteilten Karte befindet.

Welcome to Any Bank

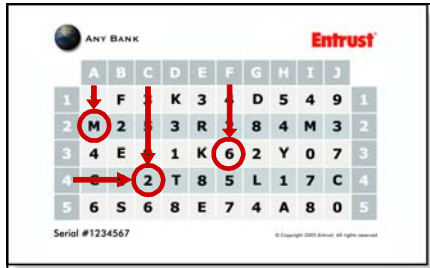
User Name:

Password:

IdentityGuard: **A2** **C4** **F3**

¹³ [Putting an End to Account-Hijacking Identity Theft](#) – Study Supplement, Federal Deposit Insurance Corporation, June 17, 2005.

Fragt das System beispielsweise nach den Zeichen an den Koordinaten A2, C4, und F3, ermittelt der Anwender die Antwort einfach durch Ablesen der Werte.



Im Beispielfall müsste er also antworten: An den Stellen A2, C4, und F3 befinden sich auf meiner Karte die Zeichen "M", "2" und "6". Bei jedem Login sucht der Server nach dem Zufallsprinzip andere Koordinaten aus, deren Inhalt er den Anwender eingeben lässt.

Grid-Authentifizierung reduziert deutlich die Gefahr, Phishing- oder Malware-Angriffen zu erliegen. Selbst wenn der Angreifer die Kommunikation zwischen Anwender und Online-Dienst mehr als einmal unterwandern kann, macht es ihm die große Zahl der möglichen Abfragekombinationen sehr schwer, bei seinen Bemühungen auf seine Kosten zu kommen. Auch die Aufzeichnung mehrerer Logins liefert dem Betrüger nämlich nur einen kleinen Teil der Karte als Ergebnis. Für einen wirklich erfolgreichen Angriff müsste er einen Aufwand treiben, der die Vorteile traditioneller Online-Angriffe ad absurdum führt.

Um das Sicherheitslevel gleich bleibend hoch zu halten, kann der Anbieter seinen Kunden regelmäßig neue Karten zukommen lassen. Ob dies alle paar Jahre oder öfter geschehen sollte, hängt vom Kontext der Anwendung ab. Weil damit keine spezielle Hardwareverteilung verbunden ist, fallen die Kosten dafür sehr gering aus.

Listen mit Einmal-Kennwörtern (TANs). Als Alternative zu Grid-Karten kommen gedruckte Listen mit Einmal-Kennwörtern (TANs) in Frage.

Nummer	TAN
00001	A 3 Ü D S T 2 3
00002	7 5 G R K Y F Z
00003	H 5 D I 9 7 D C
00004	G H G T 5 R 4 E
.....	- - - - -
00029	O S F 3 W 1 M O
00030	L B G 6 2 L M Z

Diese Kennwörter lassen sich als Teil der Anmeldeprozedur abfragen, werden aber häufig auch zur Freigabe einzelner Transaktionen verwendet. Für die Überweisungen vieler deutscher Online-Banken ist dieses Verfahren Standard.

Transferbestätigung

Sie wollen **10.000 Euro** überweisen.
Bitte bestätigen Sie die Transaktion durch Eingabe der folgenden TAN-Nummer aus Ihrer Liste:

00005: _____

Die TAN ist danach für weitere Transaktionen ungültig. Bitte streichen Sie sie aus der Liste.

Um die Anfälligkeit gegen Phishing- und Malware-Angriffen zu reduzieren, fragen viele Dienste pro Transaktion eine per Zufallsprinzip bestimmte TAN aus der aktuellen Liste des Anwenders gezielt ab. So hilft es einem Angreifer nichts, beispielsweise über eine Betrugsseite gleich mehrere aufeinander folgende TANs abzufangen, weil nicht vorherzusehen ist, welche TAN der Online-Dienst beim nächsten Kontakt verlangen wird. Die Anwender wiederum streichen die verbrauchten TANs aus ihren Listen oder erhalten von vornherein Ausdrucke, bei denen sie die erfragte TAN jeweils frei rubbeln müssen.

Die Tatsache, dass der Anbieter jede Kennwortliste nach dem Verbrauch aller TANs ersetzen muss, erfordert häufigen Briefkontakt mit aktiven Anwendern. Außerdem ist es notwendig, den TAN-Verbrauch kontinuierlich genau zu überwachen, damit den Anwendern immer rechtzeitig eine neue Liste zugestellt werden kann, bevor sie alle aktuellen TANs verbraucht haben.

Aus diesen Gründen kann der Verwaltungsaufwand für das PIN/TAN-Verfahren größer sein als der für die Grid-Authentifizierung. Entrust IdentityGuard 8.0 bietet die Methode trotzdem an, damit Anwender, die sich daran gewöhnt haben, das Verfahren weiter nutzen können.

Wissensgestützte Authentifizierung ("Shared Secrets"). Eine der einfachsten Methoden, um die Identität des Anwenders eines Online-Dienstes genauer zu bestimmen, besteht darin, ihn während des Anmeldeprozesses nach Informationen zu fragen, die nur er kennen kann. Dabei handelt es sich entweder um "geteilte Geheimnisse" – Frage-Antwort-Paare, die der Anwender während eines Registrierungsprozesses mit dem Dienst vereinbart – oder um Daten

früherer Transaktionen, die nur der Server und der Anwender kennen.

Bei einem typischen Registrierungsprozess kann der Anwender beispielsweise sein Geburtsjahr, seinen Geburtsort oder sein Lieblingshaustier angeben. Nach diesen Informationen wird er dann vor Transaktionen, die eine Authentifizierung erfordern, vom Online-Dienst gefragt.

Zusätzliche Authentifizierung

Um die Sicherheit Ihrer Identität bei Transaktionen von diesem Computer sicher zu stellen, beantworten Sie bitte folgende Fragen:

Wann wurden Sie geboren?

_____ (Liste)

Was ist Ihr Lieblings-Haustier?

_____ (Liste)

Wie hoch ist Ihre Miete?

_____ (Liste)

Für Angreifer schwieriger zu ermitteln als die genannten Beispiele sind die richtigen Antworten auf Fragen, die sich auf frühere Transaktionen beziehen: *Was war Ihr Endkontostand auf dem letzten Auszug? Wie hoch genau ist Ihre monatliche Miete?*

Entrust IdentityGuard 8.0 erlaubt es Online-Anbietern, für jeden Anwender eine ganze Reihe von Frage-Antwort-Paaren zu definieren und beim Authentifizierungsprozess jeweils alle oder einen Teil der Fragen zu stellen. Wird eine größere Zahl von Fragen festgelegt und bei den Anmeldungen jeweils ein unterschiedlicher Teil davon verwendet, hat es ein Angreifer schwerer, mit bereits erlauschten Antworten etwas anzufangen.

Geräteauthentifizierung. Eine Authentifizierung, die sich auf die Überprüfung des Anwendercomputers stützt, fordert vom Anwender selbst keine Aktivität und schützt doch gegen eine Reihe von Angriffsformen. Diese Methode ist besonders attraktiv für Umgebungen, in denen sich die Anwender normalerweise mit immer denselben Geräten bei einem Online-Dienst anmelden.

Um die Identität eines Computers zu bestimmen, wird ein so genannter "Fingerabdruck" des Rechners erstellt. Er entsteht aus Parametern, die ein Computer für Lesezugriffe offen zur Verfügung stellt – so lässt sich etwa das Land des Computerstandortes über Reverse-DNS-Lookup bestimmen, und der Computer gibt Daten wie die Betriebssystem- und Browserversion und andere individuelle Kennzeichen preis. Identität

Guard speichert diesen Fingerabdruck gegen Fremdzugriffe gesichert ab. Außerdem vergibt IdentityGuard eine Referenznummer für das Gerät, das zur Anmeldung verwendet werden soll, und legt diese per Cookie auf dem Gerät des Anwenders ab.



Bei jeder späteren Anmeldung liest IdentityGuard die Referenznummer des Anwendercomputers. Sie weist den Anwender als legitimen Nutzer aus. IdentityGuard errechnet aber auch den zugehörigen „Fingerabdruck“ neu und vergleicht ihn mit der gespeicherten Version. Nur wenn beide übereinstimmen, schließt das System den Anmeldeprozess ohne Abbruch oder weitere Authentifizierungsschritte ab.



Mit der Geräteauthentifizierung schützt IdentityGuard die Anwender eines Online-Dienstes auch dann, wenn ein Angreifer ihre Kennwörter an sich bringen konnte. Versucht sich ein Betrüger damit anzumelden, fehlen ihm immer noch die Identitätsdaten der zugehörigen Computer.

Der Einsatz der Geräteauthentifizierung bedeutet nicht, dass ein Anwender nur noch einen einzigen Computer für den Zugriff auf den geschützten Online-Dienst nutzen kann oder dass er von der Existenz des Cookies abhängig ist. IdentityGuard 8.0 lässt sich so einstellen, dass das System beim Zugriff mit einem fremden Computer oder beim Fehlen des Cookies entweder eine andere Form der starken Authentifizierung verlangt oder die Rechte des Anwenders temporär begrenzt. Außerdem kann ein Anwender mehrere Computer für die Geräteauthentifizierung registrieren.

Die Geräteauthentifizierung selbst ist gegen Angriffe unempfindlich. Auf den Cookie mit der Referenznummer des Anwender-Computers etwa kann nur die berechtigte Website zugreifen. Um dies zu erreichen, werden eingebaute Schutzfunktionen der Web-Browser benutzt. Und selbst dann, wenn es einer besonders raffiniert programmierten Malware gelingen

sollte, die Identitätsdaten eines Gerätes auszuspielen, würde dies dem Angreifer kaum helfen. Wenn er die Daten nämlich bei einem Anmeldeversuch von einem anderen Gerät aus einzusetzen versucht, stimmt immer noch nicht der Fingerabdruck.

Als zusätzlichen Sicherheitsfaktor kann IdentityGuard optional Informationen über die Transaktionsreihenfolge codiert im Cookie speichern. Jeder Cookie gilt dann nur bis zur nächsten Anmeldung. Einen kopierten Cookie kann ein Betrüger dann nicht mehr nutzen, wenn sich der rechtmäßige Anwender zwischenzeitlich beim Online-Dienst angemeldet hat. Der rechtmäßige Nutzer wiederum bemerkt einen fremden Anmeldeversuch mit gestohlenem Cookie daran, dass der Server seinen eigenen Rechner nicht sofort akzeptiert.

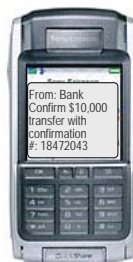
Out-of-Band-Authentifizierung (Zweiter Kanal).

Eine der sicherheitstechnischen Grundprobleme der Online-Authentifizierung ist die Tatsache, dass für die Authentifizierung und die eigentlichen Transaktionen gewöhnlich derselbe Kommunikationskanal benutzt wird. Out-of-Band-Authentifizierung greift deshalb auf einen unabhängigen Kanal zurück, um den Anwender auch dann zu schützen, wenn der primäre Kommunikationsweg bereits kompromittiert ist.

Diese Methode schützt effektiv gegen *Man-in-the-Middle*-Attacken, bei denen sich ein Angreifer in eine rechtmäßige Online-Verbindung einschaltet, als Zwischenstation die Eingaben des Anwenders abfängt und verändert an den Server weiterschickt.

Out-of-Band-Authentifizierung ist für den Anwender bequem, weil sie existierende, vertraute und leicht zugängliche Kanäle benutzt, um einzelne Transaktionen zu bestätigen.

<p>Transferbestätigung</p> <p>Sie wollen 10.000 Euro überweisen.</p> <p>Eine Bestätigungsnummer wurde an Ihr registriertes Mobiltelefon geschickt.</p> <p>Bitte geben Sie die Nummer zur Bestätigung ein: _____</p> <p style="text-align: right;"><input type="button" value="OK"/></p>
--



Entrust IdentityGuard unterstützt die Out-of-Band-Methode, indem das System bei Bedarf Einmal-Kennwörter erzeugt und zusammen mit Transaktionsinformationen über E-Mail, SMS oder Stimmgenerator und Telefon an den Anwender übermittelt. Sobald der Anwender sein Einmal-Kennwort auf einem dieser Wege erhalten und überprüft hat, ob die mitgelieferten Transaktionsdaten seinen Eingaben entsprechen, gibt er das Kennwort zur Bestätigung seiner Identität und zur Bekräftigung seines Willens in die Kommunikationsmaske des Onlinedienstes ein.

Wechselseitige Authentifizierung

Mithilfe der wechselseitigen Authentifizierung können Anwender echte von gefälschten Online-Seiten unterscheiden und deshalb noch sicherer vermeiden, betrügerischen Sites persönliche Informationen preiszugeben.

Wichtig ist dies vor allem angesichts der ständig steigenden Zahlen von Phishing-Attacken. Ein Blick auf die URL hilft dabei längst nicht mehr in jedem Fall, eine echte E-Commerce- oder Banking-Site von einer Fälschung zu unterscheiden. Ausgefeilte Angriffstechniken locken Anwender selbst dann auf gefälschte Websites, wenn sie korrekte URLs eingeben. Für die Anbieter ergibt sich daraus eine neue Anforderung: Sie müssen dafür sorgen, dass sich auch ihre Online-Seiten auf leicht verständliche Weise beim Kunden authentifizieren.

Wechselseitige Authentifizierungssysteme liefern dem Anwender während seines Zugriffs auf eine Site einfach zu überprüfende Informationen, die nur das vertrauenswürdige Anbietersystem kennen kann. Entrust IdentityGuard bietet dazu eine Reihe unterschiedlicher Optionen:

- Angabe der Seriennummer einer Grid-Karte,
- Anzeige von Koordinaten und Werten aus einer Grid-Tabelle,
- Wiedergabe von Texten und
- Wiedergabe von Bildern.

Wiedergabe von Grid-Seriennummer und Tabelleninhalten. Die Grid-Authentifizierung eignet sich vorzüglich auch für die wechselseitige Authentifizierung.

Eine Möglichkeit besteht darin, dem Anwender die individuelle Seriennummer seiner Karte zu zeigen, die nur der Aussteller und er selbst kennen können. Die Nummer kann zur Bestätigung einer korrekten Verbindung beispielsweise während des Logins angezeigt werden, noch bevor der Anwender ein Kennwort oder Daten von der Karte eintippt. Er weiß dann rechtzeitig, dass er tatsächlich mit der gewünschten Site verbunden ist.

Mutual Authentication

Your Entrust IdentityGuard serial number is **1234567**

To confirm the authenticity of this site, use your Entrust IdentityGuard to look up the following coordinates:

[E1] [F5] [I3]

You should see the following numbers:

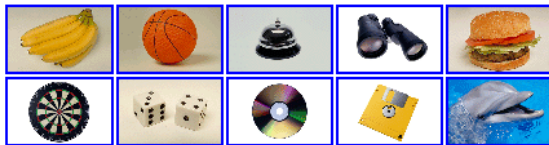
Eine andere Methode ist die Angabe von Werten, die auf der individuellen Grid-Karte des Anwenders an bestimmten Stellen stehen. Nennt der Server die richtigen Werte, weiß der Anwender, dass der Online-Dienst seine Karte kennt und sie somit ausgestellt haben muss.

Das Abfangen der Authentifizierungsdaten des Servers kann IdentityGuard zusätzlich erschweren, indem das System Zeichen verwendet, die ein Mensch gut lesen kann, eine Maschine oder ein Programm aber nicht. Außerdem kann IdentityGuard für die Authentifizierung des Online-Dienstes wiederum zusätzliche Kommunikationskanäle nutzen.

Bild- und Textwiedergabe. Für eine wechselseitige Authentifizierung ohne Grid-Karten greift IdentityGuard auf verschiedene Formen der Bild- und Textwiedergabe zurück.

Personalized Image Selection

Click on one of the images below to select it as you Entrust IdentityGuard image:



-- OR --

Upload a picture from your machine:

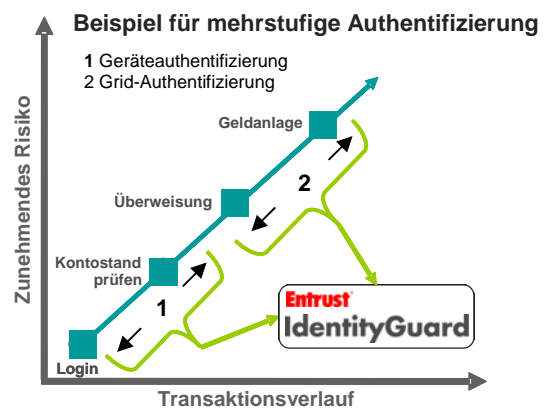
In diesem Fall sucht der Anwender zur Personalisierung des Log-In-Vorgangs bei der Registrierung ein Bild aus einer Reihe von Beispielen aus, tippt einen nur ihm bekannten Text ein oder lädt ein eigenes digitales Bild auf den Server. Nur der richtige Server kann später die entsprechenden Informationen anzeigen. Geschieht dies bereits vor der Angabe persönlicher Informationen oder Kennwörter, weiß der Anwender auch in diesem Fall früh genug, ob er mit der korrekten Site verbunden ist. Sowohl ausgewählte als auch individuell übertragene eigene Bilder haben den Vorteil, dass sie sich leicht erkennen und merken lassen und dass ihr Fehlen schnell auffällt – etwa dann, wenn eine Phishing-Site persönliche Daten abfragen will, das gewohnte optische Umfeld der zugehörigen Webseite aber fehlt.

Risikogesteuerte Sicherheit

Mit Entrust IdentityGuard 8.0 lassen sich die Anmeldeprozeduren eines Online-Dienstes risikoabhängig auswählen und steuern. Der Anwender trifft dann je nach Verbindung oder Transaktion auf die größtmögliche Bequemlichkeit, aber immer auch auf angemessene Sicherheitsmaßnahmen.

Das umständliche Handling von Hardware-Tokens etwa lohnt sich nicht, wenn es nur darum geht, Kunden die Online-Überprüfung von Kontoständen zu ermöglichen. Ein Angreifer könnte in diesem Fall nämlich schlimmstenfalls den Kontostand sehen. Andererseits ist Kennwort-Authentifizierung zu schwach, wenn es um die Absicherung von Überweisungen hoher Beträge geht. Der Schaden, den ein Betrüger anrichten kann, rechtfertigt in diesem Fall aufwändigere Maßnahmen.

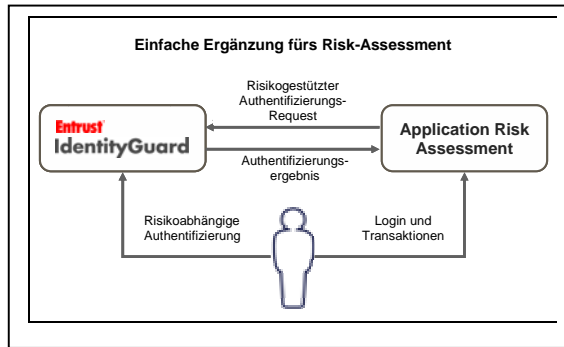
Alle von Entrust IdentityGuard angebotenen Authentifizierungsmethoden lassen sich bei der Anmeldung an einem System nacheinander oder gleichzeitig einsetzen. Wie im folgenden Bild dargestellt, reicht für den Konto-Check vom heimischen PC aus oft schon die Geräteauthentifizierung. Will derselbe Kunde aber Geld anweisen, um eine Rechnung zu bezahlen, ist eine zusätzliche Grid-Authentifizierung sinnvoll. Auf diese Weise läuft die reine Kontoüberprüfung schnell und für den Kunden ohne unnötige Barrieren ab, während die höherwertige und risikoreichere Transaktion einen adäquaten, aber immer noch benutzerfreundlichen Schutz genießt.



Flexible Richtliniengestaltung

Entrust IdentityGuard 8.0 macht richtliniengestützte Authentifizierung leicht. Besonders einfach ist die Durchsetzung einer Policy, die bestimmte Transaktionen unabhängig vom Anwender generell einer höheren Risikostufe zuordnet. Eine Bank etwa könnte alle Überweisungen von einem Wert über 10.000 Euro

entsprechend rubrizieren und dafür mehr als eine bloße Kennwort-Authentifizierung verlangen.



IdentityGuard 8.0 lässt sich darüber hinaus an bereits vorhandene Verfahren und Produkte koppeln, die nach Verhaltensmustern von rechtmäßigen Benutzern einerseits und Betrügern andererseits suchen. Meldet sich ein Anwender beispielsweise für eine Überweisung von einem registrierten Gerät aus an, kann dies eine hilfreiche Information zur Einschätzung des Risikos darstellen. IdentityGuard stellt deshalb Daten über den aktuellen Authentifizierungsprozess auf Wunsch einem Risk-Assessment-System zur Verfügung.

Andererseits kann ein Risk-Assessment-System von IdentityGuard einen zusätzlichen Authentifizierungsschritt verlangen, wenn etwa eine Überweisung nicht zur Transaktionshistorie und zum Profil eines bestimmten Anwenders passt.

Akzeptanz durch Benutzerfreundlichkeit

Entrust IdentityGuard 8.0 passt sich auf einfache Weise den Gewohnheiten und Erwartungen der Anwender an, erhöht damit die Akzeptanz und verringert den Support-Aufwand. Keine der Authentifizierungsmethoden des Systems erfordert eine Hard- oder Softwareverteilung an die Endanwender. Dies senkt nicht nur die Einführungskosten, sondern erhöht auch die Bequemlichkeit beim täglichen Einsatz:

Grid-Authentifizierung. Die Grid-Tabellen können als einfache Plastikkarten gestaltet oder direkt auf ohnehin vorhandene Kredit- oder Bankkarten gedruckt werden. Die Verteilungsmechanismen und die Form sind somit die gleichen wie bei den vertrauten Karten, die der Anwender leicht jederzeit bei sich tragen kann. Mit der Karte selbst schließlich kommen die Besitzer intuitiv zurecht: Unabhängige Usability-Tests haben ergeben, dass 94 Prozent der eingesetzten Testpersonen mit unterschiedlichem Alter und unter-

schiedlicher Lebenserfahrung die Karten sofort ohne fremde Hilfe benutzen konnten.¹⁴

Wissensgestützte Authentifizierung. Frage-Antwort-Paare lassen sich direkt bei der Registrierung eines Anwenders für einen Online-Dienst im Dialog mit ihm individuell festlegen. Ob auf Details wie Groß- und gegebenenfalls selbst fest. Da er während der Authentifizierung nur nach Informationen gefragt wird, die er ohnehin kennt, muss er sich – im Gegensatz zum Kennwort-Konzept – keine zusätzlichen Daten merken.

Geräteauthentifizierung. Den Fingerabdruck des Computers, den der Anwender benutzt, ermittelt Entrust IdentityGuard 8.0 transparent während einer Online-Sitzung. Wiederum muss weder Hard- noch Software an den Endanwender übermittelt werden. Auch die eigentlichen Authentifizierungsvorgänge laufen in diesem Fall ab, ohne dass der Anwender aktiv werden muss. Die Registrierung eines neuen Computers kann IdentityGuard beispielsweise durch wissensgestützte Authentifizierung absichern.

Out-of-Band-Authentifizierung (Zweiter Kanal). Wie die Geräteauthentifizierung nutzt diese Methode Hardware, die sich schon in den Händen der Anwender befindet. Die Kunden empfangen ihre Einmal-Kennwörter bequem über Festnetz- oder Mobiltelefon, PDAs oder beliebige E-Mail-Accounts.

Entrust IdentityGuard erlaubt die Personalisierung von Authentifizierungsmethoden. Die Flexibilität von Entrust IdentityGuard macht es Organisationen möglich, bei Authentifizierungsvorgängen auch auf persönliche Vorlieben ihrer Kunden einzugehen – so bevorzugt der eine vielleicht die Übertragung von Einmalkennwörtern per SMS, während der andere lieber einen Anruf wünscht. Lässt es das Risikolevel zu, können Anwender frei zwischen verschiedenen Verfahren wählen – etwa zwischen wissensgestützter Authentifizierung und Grid-Karte. Die Wahlfreiheit verringert die Gefahr, dass sich Kunden abwenden, weil sie mit den Authentifizierungsvorgängen eines Online-Dienstes nicht zufrieden sind.

Einfache und kostengünstige Einführung

Entrust IdentityGuard reduziert die Einführungskosten für starke Authentifizierung durch leichte Integration in existierende Infrastrukturen und durch die geringen Kosten seiner Authentifizierungstechniken. Angesichts des wachsenden regulatorischen Drucks und des schwindenden Konsumentenvertrauens wächst der Druck auf Online-Anbieter, starke Authentifizierung beschleunigt einzuführen. Entrust IdentityGuard 8.0 erleichtert dies, weil das

¹⁴ Entrust IdentityGuard Usability Testing, Design Interpretative, June 2005.

System erheblich geringere Einführungs- und Wartungskosten bietet als beispielsweise zeitsynchrone Hardware-Tokens. Ein wichtiger Grund für den Kostenvorteil ist, dass bei den Endanwendern weder Hard- noch Software implementiert und gepflegt werden muss. Weitere Vorteile liegen darin, dass existierende Anwendungen weiter laufen können, und dass eine Ausweitung der Authentifizierung auf Telefon oder ATM/Kiosk-Applikationen möglich ist.

Preiswerte Authentifizierungsmittel

Konventionelle zeitsynchrone Hardware-Tokens sind um das Mehrfache teurer als die Authentifizierungstechniken, die Entrust IdentityGuard 8.0 nutzt¹⁵. Dies hängt auch mit versteckten Kosten zusammen, die bei der Evaluierung selten bedacht werden:

- **Softwareserver-Kosten.** Viele Token-Anbieter verstecken signifikante Kostenfaktoren in ihren Server-Komponenten. Die jeweiligen Lizenz- und Wartungskosten müssen deshalb genau analysiert werden.
- **Servicekosten.** Nach dem Kauf ergeben sich oft hohe jährliche Servicekosten über die reinen Lizenzkosten hinaus. Ein Beispiel sind Verifikationskosten: Manches System generiert jedes Mal eine Transaktionsgebühr, wenn eine Token-Authentifizierung überprüft wird.
- **Wiederbeschaffungskosten.** Speziell bei Hardware-Tokens spielen die Wiederbeschaffungskosten bei Fehlern und Ausfällen eine große Rolle. Dabei ist nicht nur der Kauf der neuen Tokens, sondern auch der Aufwand für deren Weitergabe an die Kunden zu bedenken.

Keine der von Entrust IdentityGuard verwendeten Authentifizierungsmethoden erfordert die Distribution von Hard- oder Software. Das System greift auf das Wissen der Kunden und existierende Hardware zurück oder nutzt – im Falle der Grid-Karten – extrem kostengünstige Formfaktoren. All dies bedeutet für Online-Anbieter die Chance, starke, wechselseitige Authentifizierung bei signifikant reduziertem Kostenaufwand einzuführen.

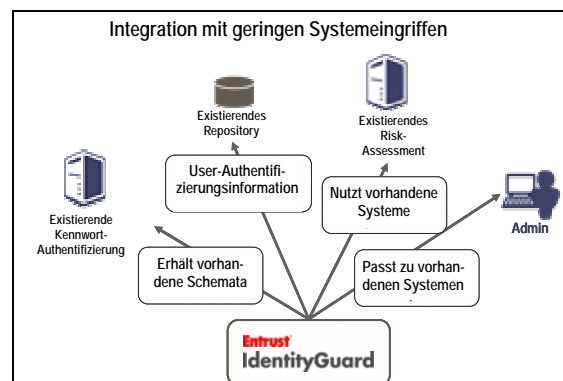
Integration ohne tiefe Systemeingriffe

Die meisten Online-Anbieter haben bereits viel Geld in Infrastruktur investiert – auch in Kennwort-Infrastrukturen, Anmeldeverfahren, Anwenderdatenbanken und administrative Prozesse. Angesichts des Drucks, schnell auf stärkere Authentifizierungsverfahren umzusteigen, sehen sich die Unternehmen mit einem Zwang zu unverhältnismäßig kostenrächtigen und risikoreichen Eingriffen in ihre existierenden Systeme konfrontiert.

¹⁵ [Entrust IdentityGuard Total Cost of Ownership Calculator](#)

Um dies zu verhindern, arbeitet Entrust IdentityGuard mit vorhandenen Infrastrukturen zusammen:

- Das System verwendet bestehende Schemata für Användernamen und Kennwörter weiter,
- es nutzt bereits vorhandene Anwenderverzeichnisse und Datenbanken für die Authentifizierungsinformationen,
- es bedient sich bereits laufender Anomalie- und Betrugserkennungssysteme und versorgt diese im Gegenzug mit Informationen zu Authentifizierungsprozessen und
- es integriert sich über Management-APIs in vorhandene Verwaltungsprozesse.



Alternative Ansätze zur Einführung stärkerer Authentifizierung warten oft mit erheblichen Kosten auf und erweisen sich als kompliziert. In einigen Fällen etwa erfolgt eine derart enge Verzahnung der Authentifizierung mit Betrugserkennungssystemen, dass für den Betrieb hoch komplexe Zugriffsregeln aufgestellt werden müssen. Diese überschneiden sich häufig mit denen vorhandener Applikationen und blockieren dann unabsichtlich legitime Anwender. Das Resultat sind Anrufe beim Helpdesk und abgebrochene Transaktionen.

Systeme mit künstlicher Intelligenz verlangen oft lange Trainingszeiten. Während dieser Zeit deuten sich berechnete Zugriffe häufig fälschlicherweise als betrügerisch, was die rechtmäßigen Anwender verärgert.

Auch Identity-Federation-Ansätze können die Einführung von starker Authentifizierung unnötig komplizieren. Die Idee dazu haben ursprünglich die Hersteller von Hardware-Tokens entwickelt. Sie suchten ein Mittel gegen negative Anwendererfahrungen, die aus der wachsenden Zahl bei sich zu tragender Tokens erwachsen. Identity Federation kann Abhängigkeit von Dritten bedeuten, denn die Authentifizierung muss in diesem Fall mit den Services von

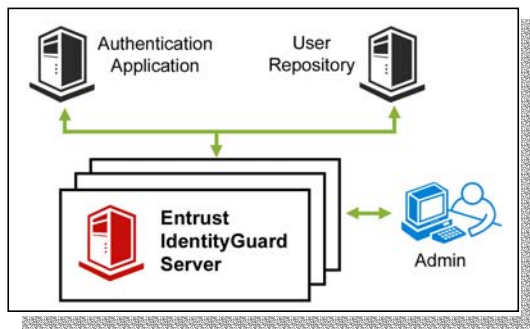
Dienstleistern oder sogar Konkurrenten zusammenarbeiten. Dies hat nicht nur Auswirkungen auf die technische Infrastruktur. Es hat auch zur Folge, dass der Anwender im Fall von Problemen mit dem Authentifizierungssystem nicht genau weiß, bei wem er Hilfe bekommt. Digitale Anmeldeverfahren, die ohne Hardware beim Endanwender auskommen, machen Identity-Federation-Ansätze unnötig.

Mehrkanal-Authentifizierung

Entrust IdentityGuard 8.0 wurde so gestaltet, dass sich das System unterschiedlicher Authentifizierungskanäle bedienen kann – darunter Telefon, Geldautomaten und Authentifizierung beim persönlichen Besuch am Schalter. Dies ist möglich, weil das Produkt anstelle komplizierter User-Interfaces lediglich eine einfache Tastatur als Eingabeinstrument erfordert. So lässt sich IdentityGuard beispielsweise für die Authentifizierung während der Kommunikation mit einem Callcenter verwenden. Der Anrufer gibt in diesem Fall die Werte auf seiner Grid-Karte direkt in die Tastatur seines Tonwahl-Telefons ein. Die Möglichkeit, das System für mehrere Kanäle zu verwenden, schützt zusätzlich die Investition in Entrust IdentityGuard.

Architektur und Integration

Entrust IdentityGuard 8.0 wurde so programmiert, dass das System mit Authentifizierungs-Infrastrukturen zusammenarbeitet, wie sie typischerweise von Online-Anbietern verwendet werden. Bei der Implementierung sind kaum Eingriffe in existierende Systeme notwendig. Hinzu kommt, dass das System auf hohe Skalierbarkeit ausgelegt ist.



Integration mit geringem Aufwand

Entrust IdentityGuard unterstützt sowohl Eigenentwicklungen von Kunden als auch Web-Access-Control-Produkte anderer Hersteller. Im allen Fällen erlaubt es IdentityGuard, gezielt einen zweiten Authentifizierungsfaktor ins Spiel zu bringen. Nahezu alle bekannten Produkte für die Zugriffskontrolle auf Websites stellen zu diesem Zweck ein Standard-Interface zur Verfügung.

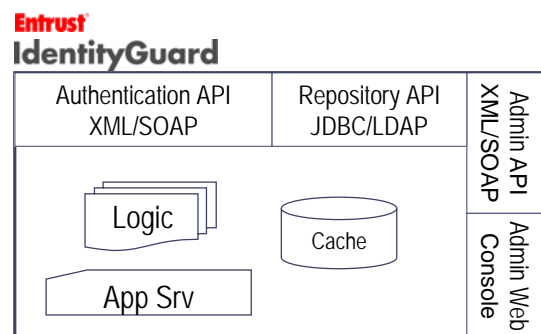
Das Authentifizierungsinterface nutzt entweder Java oder Webservices, um den Anforderungen von Authentifizierungsapplikationen sowohl unter J2EE als auch .NET gerecht zu werden. Bei den meisten Transaktionen wird es darum gehen, dass eine Applikation den Authentifizierungsversuch eines gegebenen Anwenders zur Verifizierung weiterreicht. Sobald die Verifizierung gelungen ist, liefert der IdentityGuard-Server das Ergebnis.

Entrust IdentityGuard nutzt vorhandene Repositories für Anwenderdaten. Repositories dienen dazu, Authentifizierungsinformationen einzelner Anwender zu speichern. Wenn für einen bestimmten Anwender eine Grid-Karte ausgestellt wird, sichert IdentityGuard die Karteninformationen verschlüsselt im Repository. Diese Daten liest IdentityGuard jedes Mal, wenn es einen Anwender authentifiziert. Das zugehörige Interface unterstützt LDAP, Active Directory, JDBC und kundenspezifische APIs.

Schließlich ist ein Interface zur Remote-Administration vorhanden, über das sich die verschiedenen Funktionen zur Verwaltung der Anwender und der Authentifizierungsmethoden steuern lassen. Per API stehen die Verwaltungsfunktionen auch Systemen zur Verfügung, die dem Anwender-Identitätsmanagement und dem Provisioning dienen.

Robuste, flexible Architektur

Entrust IdentityGuard ist hoch skalierbar, um den Anforderungen von Applikationen für Konsumenten mit einer hohen Zahl an Transaktionen zu entsprechen. Aus diesem Grund unterstützt das Produkt die Verteilung auf mehrere Server in einer Load-Balancing-Umgebung. Dieses Feature macht es außerdem möglich, den Durchsatz bei Bedarf durch weitere Server zu erhöhen. Ein High-Performance-Cache für Anwenderinformationen beschleunigt Transaktionen zusätzlich.



Die Entrust-IdentityGuard-Plattform basiert auf einem Server-gestützten Software-Produkt, das in typischen Unternehmensinfrastrukturen installiert werden kann.

Es handelt sich um eine J2EE-Applikation, die in Java geschrieben wurde und auf einem Linux-Betriebssystem läuft. Die Sicherheits-Operationen für die Erstellung, Verschlüsselung und Entschlüsselung von Karteninhalten nutzen die nach Common-Criteria und FIPS 140-2 zertifizierte Verschlüsselungssoftware von Entrust. Der Erstellungsprozess der Authentifizierungsdaten ist auf diese Weise hervorragend abgesichert. Nicht einmal Angreifer, die sich bereits Zugriff auf die Infrastruktur des Online-Anbieters verschafft haben, können sich an den Informationen im Repository zu schaffen machen.

Wie alle Entrust-Produkte unterliegt IdentityGuard hohen Standards in den Bereichen Entwicklung, Qualitätssicherung und Sicherheit. Käufer werden rund um die Uhr durch weltweiten 24x7-Service und Support unterstützt.

Zusammenfassung

Steigende Zahlen bei Fällen von Identitätsbetrug zwingen Online-Anbieter dazu, aktiv und mit hoher Priorität Systeme für starke Authentifizierung einzuführen. Diese Systeme müssen allerdings einfach zu nutzen sein und sollen weniger Kosten verursachen als traditionelle Produkte wie zeitsynchrone Hardware-Tokens.

Entrust IdentityGuard 8.0 kommt diesen Wünschen als flexible, risikogesteuerte Authentifizierungsplattform entgegen. Online-Anbieter haben die Möglichkeit, mit Entrust IdentityGuard auch einer größeren Nutzerzahl eine starke Authentifizierung zu vertretbaren Kosten zur Verfügung zu stellen. Flexibilität in der Anpassung an die Bedürfnisse unterschiedlicher Kunden und Transaktionen ist dabei eine besondere Stärke des Produkts, denn es kann seine Authentifizierungsfunktionen dynamisch dem jeweiligen Anwendungskontext anpassen. Eine Verteilung von Hard- oder Software an die Anwender ist nicht notwendig.

Mehr Informationen zu Entrust IdentityGuard finden Sie unter <http://www.entrust.com/IdentityGuard/>.

Über Entrust

Entrust, Inc. [NASDAQ: ENTU] ist ein weltweit führender Anbieter von sicheren Identity- und Access-Management-Lösungen. Mehr als 1.400 Organisationen in über 50 Ländern setzen die bewährten Softwarelösungen und Services von Entrust ein. Die Software von Entrust ermöglicht es Mitarbeitern, Kunden und Partnern, auf Unternehmensanwendungen zuzugreifen, ohne dass Sicherheitslücken entstehen. Sicheres Identity-Management, sicheres Messaging und Datensicherheit schützen die Abwicklung von Online-Transaktionen und steigern zudem die Produktivität. Weitere Informationen finden Sie unter www.entrust.com

Weiterführende Texte

[Anti-Phishing Working Group, August 2005 Activity Report, Computer Security Industry Association.](#)

[Entrust IdentityGuard Strong Authentication Solution Information](#)

[Entrust IdentityGuard Total Cost of Ownership Calculator](#)

[Entrust Online Banking Security Survey](#), October 2005.

[Entrust Internet Security Survey](#), September 2004.

[Entrust Security Survey](#), April 2005.

[FDIC Financial Institution Letter FIL-103-2005](#), October 12, 2005.

[FSTC Counter-Phishing Initiative](#), December 2004.

[Gartner Security Survey](#), 23 June 2005.

[Putting an End to Account-Hijacking Identity Theft – Study Supplement](#), Federal Deposit Insurance Corporation, June 17, 2005.

[Putting an End to Account-Hijacking Identity Theft](#), FDIC, 14 December 2004.