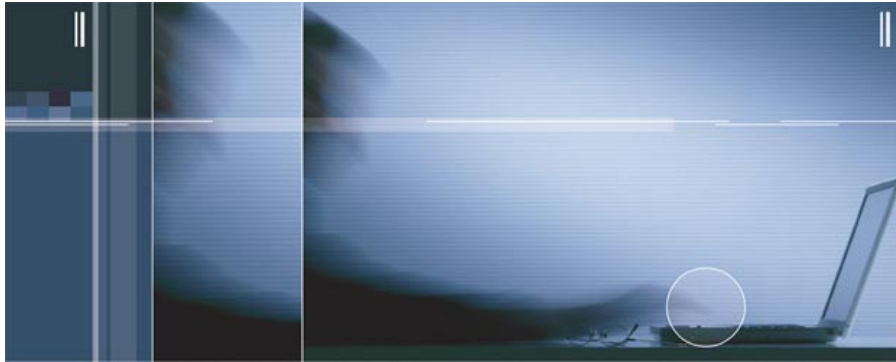


**Entrust**<sup>®</sup> Securing Digital Identities & Information



**Securing Your  
Digital Life**

**Schutz vor Online Identity Theft**  
*Neue Werkzeuge zur Bekämpfung von Identity Theft im Internet*

Februar 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 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

<b>EINFÜHRUNG .....</b>	<b>1</b>
<b>DIE KRISE DER ONLINE IDENTITY .....</b>	<b>1</b>
SCHNELLE ZUNAHME VON IDENTITY THEFT .....	1
PHISHING-ATTACKEN WERDEN ALLTÄGLICH .....	1
ÄNGSTE DER BENUTZER SCHRÄNKEN ONLINE-HANDEL EIN .....	2
ABWEHR DER BEDROHUNG .....	2
<b>ENTRUST IDENTITYGUARD – SCHUTZ VOR ONLINE IDENTITY THEFT .....</b>	<b>3</b>
SICHERE UND DOCH EINFACHE AUTHENTIFIZIERUNG .....	3
ABWEHR KOMPLEXERER IDENTITY THEFT-ATTACKEN .....	4
MULTI-CHANNEL-AUTHENTIFIZIERUNG .....	6
<b>EINFACHE, KOSTENGÜNSTIGERE ANWENDUNG .....</b>	<b>6</b>
ANWENDUNG .....	6
NIEDRIGERE KOSTEN FÜR DIE LAUFENDE VERWALTUNG .....	7
<b>ARCHITEKTUR UND INTEGRATION .....</b>	<b>7</b>
UNKOMPLIZIERTE INTEGRATION .....	8
STABILE, FLEXIBLE ARCHITEKTUR .....	8
<b>ZUSAMMENFASSUNG .....</b>	<b>9</b>

## Einführung

Durch das Internet ist es für Unternehmen möglich geworden, Prozesse online abzuwickeln. Dadurch können sie nicht nur neue Dienstleistungen anbieten, sondern auch ihre Kosten senken. Mit dieser Möglichkeit sind jedoch auch Risiken verbunden, insbesondere wenn geeignete Sicherheitsmaßnahmen zum Schutz der Online Identities (im Internetverkehr verwendete Identitäten) der Benutzer fehlen.

Heutzutage verzeichnen Unternehmen eine rapide Zunahme von Identity Theft (Identitätsdiebstahl oder Identitätsbetrug). Angaben der US-Handelsbehörde Federal Trade Commission zufolge ist Identity Theft die am schnellsten zunehmende Verbrechenart Amerikas mit geschätzten Verlusten von mehreren Milliarden Dollar jährlich.<sup>1</sup> Von einem ähnlichen Anstieg dieser Angriffe sind Unternehmen auf der ganzen Welt betroffen. Im Internet treten diese Angriffe z. B. in Form von Phishing auf, was zu einer schnellen Ausbreitung von Online Identity Theft führt.

Diese Angriffe stellen für Unternehmen wegen der finanziellen Verluste, die mit Identitätsdiebstahl verbunden sind, ein ernst zu nehmendes Risiko dar. Noch schlimmer ist, dass die Benutzer dadurch das Vertrauen in den elektronischen Handel verlieren, so dass die Unternehmen die Vorteile, die Online-Transaktionen im Vergleich zu den traditionellen Transaktionen haben, nicht mehr erkennen.

Deshalb ist es für jedes Unternehmen, das das Internet zur Erweiterung seiner Dienstleistungen für Kunden und Geschäftspartner nutzen will, unerlässlich, Maßnahmen zu ergreifen, um die Zunahme des Online Identity Theft zu verhindern. In diesem Artikel werden die Probleme aufgezeigt und neue Werkzeuge zur Bekämpfung der Bedrohung vorgestellt.

## Die Krise der Online Identity

Unternehmen nutzen das Internet immer mehr, um ihre Kunden und Geschäftspartner zu erreichen. Für den Benutzer kann das Internet eine bequemere Art darstellen, um Dienstleistungen in Anspruch zu nehmen und Geschäfte abzuwickeln. Für das Unternehmen kann die Nutzung des Internets einen Wettbewerbsvorteil bedeuten, indem es durch die Nutzung von Online-Methoden im Gegensatz zu den traditionellen papierbasierten Methoden Kosten spart.

Voraussetzung für den elektronischen Handel sind gegenseitig bestätigte Identitäten. Die Benutzer müssen sich darauf verlassen können, dass ihr Vertragspartner tatsächlich das angezeigte Unternehmen ist. Ebenso muss das Unternehmen darauf vertrauen können, dass die Identität des Benutzers richtig ist. Ohne dieses Vertrauen ist es wegen des hohen Risikos falscher

Angaben und betrügerischer Handlungen schwierig, Online-Geschäfte abzuwickeln.

In der Vergangenheit war eine Authentifizierung durch Benutzernamen und Passwort ausreichend, um die Anforderungen vieler E-Commerce-Transaktionen zu erfüllen. Die schnelle Zunahme des Online Identity Theft zeigt jedoch, dass Passwörter allein keinen ausreichenden Schutz vor komplexeren Identity Theft-Attacken mehr bieten.

## Schnelle Zunahme von Identity Theft

**Identity Theft ist eines der am schnellsten zunehmenden Verbrechen der Welt.** Die US-amerikanische Federal Trade Commission schätzt, dass 9,9 Millionen Amerikaner im letzten Jahr Opfer von Identity Theft wurden und dadurch ca. 5 Mrd. USD verloren haben.<sup>2</sup> In Großbritannien betrifft Identity Theft jedes Jahr über 100.000 Menschen und verursacht Kosten in Höhe von 2,4 Mrd. USD.<sup>3</sup>

Diese schnelle Zunahme von Identity Theft beruht auf verschiedenen Verbrechenarten. In einigen dieser Fälle wird die Identität einer Person gestohlen, indem sich der Täter Zugang zu Papierdokumenten verschafft und die entsprechenden Informationen zur Erstellung einer falschen Identität als Duplikat der richtigen Identität nutzt. Anschließend verwendet der Dieb die gestohlene Identität, um an Guthabeninformationen heranzukommen, Geld von Bankkonten abzuheben usw..

In anderen Fällen versucht ein Identitätsdieb, Angaben zur Online Identity zu stehlen, um sich Zugang zu den Online-Konten des Opfers, z. B. seinem Bankkonto, zu verschaffen. Sobald der Dieb auf das Bankkonto des Opfers zugreifen kann, überweist er Geld von dem Konto und beschafft sich zusätzliche persönliche Informationen, um weitere kriminelle Handlungen zu begehen. Diese Art von Identity Theft ist sehr Besorgnis erregend, da sich der Täter bzw. Dieb nicht in derselben Gegend wie das Opfer aufhalten und keinen Zugang zu Papierdokumenten haben muss. Von praktisch jedem Ort der Welt braucht der Dieb den Benutzer nur durch einen Trick zur Preisgabe seines Passworts verleiten.

## Phishing-Attacken werden alltäglich

**Wer sich auf Passwörter verlässt, trägt zur Ausweitung des Online Identity Theft bei.** Phishing-Attacken basieren auf manipulierten E-Mails und betrügerischen Websites. Sie sind so aufgebaut, dass sie die Empfänger trickreich dazu verleiten, ihren Benutzernamen und ihr Passwort preiszugeben. Diese können dann verwendet werden, um Zugang zu den Konten des Opfers zu erhalten.

Im Jahr 2003 schätzte das Marktforschungsunternehmen Gartner die Verluste durch Phishing-Attacken auf über 1,2 Mrd. USD<sup>4</sup>. Nach Angaben der Anti-Phishing Working Group (Arbeitsgruppe zur Bekämpfung von Phishing-Attacken) gab es 2004 in einem Dreimonatszeitraum über 4.500 verschiedene Phishing-Attacken mit einer Zunahme von 50% pro Monat.

---

<sup>2</sup> US Federal Trade Commission, September 2003.

<sup>3</sup> <http://www.crimereduction.gov.uk/fraud17.htm>

<sup>4</sup> Gartner, Juli 2003

<sup>1</sup> US Federal Trade Commission, September 2003.

Phishing-Attacken basieren auf der Nachmachung der vertrauenswürdigen Marken bekannter Banken, Online-Händler und Kreditkartenunternehmen in E-Mails an potenzielle Opfer, in denen die Empfänger aufgefordert werden, gefälschte Websites zu besuchen. An dieser Stelle wird der Benutzer aufgefordert, seinen Benutzernamen und sein Passwort in einem scheinbar ordnungsgemäßen Anmeldedialog einzugeben. Den Angreifern gelingt es, eine bedeutende Anzahl von Empfängern dazu zu verleiten, die Anweisungen in der E-Mail zu befolgen und ihre Benutzerinformationen preiszugeben. Diese können dann dazu verwendet werden, um sich weitere persönliche Informationen bei denselben Banken, Händlern und Kreditkartenunternehmen zu beschaffen. Die Angreifer versuchen also durch „Phishing“ (Kunstwort aus Password und fishing), an Online-Zugangsdaten heranzukommen.

Diese Angriffe werden hauptsächlich durch die Schwachstellen bei der passwortbasierten Authentifizierung möglich gemacht. Sobald ein Online-Dieb bzw. *Phisher* einen Benutzer dazu verleitet, seinen Benutzernamen und sein Passwort einzugeben, kann er auf das Online-Konto des Opfers zugreifen. Eine Attacke kann von jedem Ort der Welt ausgehen, der Dieb muss den Benutzer nur dazu bringen, seinen Benutzernamen und sein Passwort auf der gefälschten Website einzugeben. Bei einer sehr großen Anzahl von Verbrauchern, die eine solche E-Mail erhalten, ist die Wahrscheinlichkeit groß, dass sie auf diese Art von Angriff hereinfallen.

Sobald er online ist, kann ein Angreifer Kreditkarten beantragen, Zahlungsempfänger speichern, Überweisungen vornehmen und zusätzliche persönliche Benutzerdaten erhalten oder ändern. Nachdem die Phishing-Attacken jeden Monat um über 50% zunehmen, sind die potenziellen Folgen für jedes Online-Unternehmen und seine Benutzer erheblich und dürfen nicht außer Acht gelassen werden.

## Ängste der Benutzer schränken Online-Handel ein

**Es gibt jedoch Potenzial für diejenigen, die das Vertrauen der Benutzer stärken können.** Eine unausweichliche Folge der Zunahme des Online Identity Theft ist, dass die Bereitschaft der Benutzer, das Risiko der Nutzung von Online-Diensten ohne einen besseren Schutz ihrer Online Identity einzugehen, sinkt. Das bringt für die Unternehmen zwei negative Folgen mit sich: Zum einen die steigenden direkten Kosten der Angriffe und zum anderen die eingeschränkte Nutzung der Online-Dienste, die sich sowohl auf die Kosten als auch auf die Umsätze auswirken kann.

Gleichzeitig werden diejenigen Unternehmen, die dieses Problem angehen und den Benutzern einen besseren Schutz ihrer Online Identity bieten, entscheidend belohnt. Gemäß einer von Entrust durchgeführten Umfrage über Sicherheit im Internet würden 68% der Verbraucher, die zwar im Internet einkaufen, aber ihre Bankgeschäfte nicht

online abwickeln, Online-Banking wahrscheinlich in Betracht ziehen, wenn es einen besseren Schutz ihrer Online Identity gäbe.<sup>5</sup> Auch von den Benutzern, die heute Online-Banking nutzen, gaben über 90% an, dass sie höherwertige Leistungen in Anspruch nehmen würden, wenn es einen besseren Schutz ihrer Identität gäbe.

Unternehmen, die das Problem des Online Identity Theft lösen können, scheinen also einen entscheidenden Wettbewerbsvorteil zu haben. Um dies erfolgreich umzusetzen, wird eine Methode benötigt, die mehrere Faktoren berücksichtigt, darunter die Sicherheit, die Kosten und die Benutzerfreundlichkeit.

## Abwehr der Bedrohung

Bei der Abwehr des Online Identity Theft sind drei Schlüsselbereiche zu berücksichtigen:

- **Entdeckung.** Dies bedeutet, dass das Internet beobachtet werden muss, um Identity Theft-Attacken schnell festzustellen. Normalerweise umfasst dies die Beobachtung des E-Mail-Verkehrs, um gesendete Phishing-E-Mails aufzuspüren, sowie das Durchsuchen des Internets nach gefälschten Seiten. Das ist wichtig für eine schnelle Reaktion, um einen Angriff zu stoppen und seine Auswirkungen so gering wie möglich zu halten.
- **Reaktion.** Sobald ein Angriff festgestellt wurde, ist es wichtig, schnell zu handeln, um die gefälschte Seite, die dazu genutzt wird, Informationen über die Identität der Benutzer auf unrechtmäßige Weise zu beschaffen, so schnell wie möglich abzuschalten. Ebenso werden viele Unternehmen Hinweise zu Angriffen dieser Art auf ihren eigenen Websites veröffentlichen, um die Benutzer zu warnen. Normalerweise geschieht dies in Zusammenarbeit mit der Community des Internetproviders.
- **Schadensminderung.** Die Minimierung der Auswirkungen eines Angriffs, wenn er tatsächlich eintritt, ist eine der wichtigsten Maßnahmen zur Schadensbegrenzung, sowohl finanziell als auch im Hinblick auf das Vertrauen der Benutzer. In der Vergangenheit stellte die Schadensminderung auch eine der größten Herausforderungen in Bezug auf die Entwicklung einer Methode, die erfolgreich umgesetzt werden kann, dar.

Die Aufklärung der Benutzer ist ebenfalls ein wichtiger Teil eines Plans zur Schadensminderung. Online Identity Theft, der durch Phishing verübt wird, ist nur durch die Tatsache möglich, dass es den Dieben gelingt, einzelne Benutzer dazu zu verleiten, ihr Passwort offen zu legen. Obwohl die verstärkte Aufklärung der Benutzer über Phishing zur Eindämmung von Identity Theft beitragen wird, ist es unwahrscheinlich, dass Aufklärung allein ausreichend sein wird, insbesondere im Verbraucherbereich, zumal die Phishing-Attacken immer ausgereifere Formen annehmen. Deshalb muss jede Strategie zur Schadensminderung die Sicherheit unter Berücksichtigung der Tatsache verbessern, dass die Benutzer auch weiterhin

---

<sup>5</sup> Umfrage „[Entrust Internet Security Survey](#)“, September 2004

trickreich dazu verleitet werden, Informationen, die den Diebstahl ihrer Online Identity ermöglichen, offen zu legen.

Das ist eine der Beschränkungen der Systeme zur Authentifizierung des Absenders von E-Mails. Sie ermöglichen zwar ein größeres Vertrauen in die Identität des Absenders einer E-Mail, ihre durchgehende Umsetzung wird jedoch noch Jahre dauern. Außerdem ist dieses System stark davon abhängig, dass die Benutzer immer die richtigen Entscheidungen treffen. Darüber hinaus verbreiten sich kompliziertere Attacken wie Trojaner nicht unbedingt über E-Mails.

Abgesehen von der Sicherheit selbst sind Überlegungen wie Kostensenkungen und Benutzerfreundlichkeit bei der Bewertung einer Methode entscheidend. Wenn der Schutz der Online Identity eines Benutzers das Unternehmen wesentlich mehr kostet als das Unternehmen durch Identity Theft verliert, dann ist es schwierig, Argumente für die Ergreifung von Maßnahmen zu finden. Ebenso hat eine Methode, die für den Schutz der Identität der Benutzer eingeführt wird, ihren Zweck verfehlt, wenn sie so schwer zu bedienen ist, dass die Benutzer damit nicht zurechtkommen. Alle drei Kriterien sollten bewertet werden, um festzustellen, ob eine bestimmte Lösung geeignet ist.

In diesem Artikel werden die Methoden für eine aktive Schadensminderung erörtert, wobei der Schwerpunkt auf einer Lösung liegt, die erhöhten Schutz bei minimalem Kosten- und Zeitaufwand ermöglicht.

## Entrust IdentityGuard – Schutz vor Online Identity Theft

Die Entrust IdentityGuard™ Lösung, die auf einer patentierten Abfrage- und Antworttechnik beruht, bietet eine erhöhte Sicherheit und einen Schutz der Online Identities und verbessert dadurch den Schutz vor Attacken wie z. B. Phishing. Diese Lösung wurde entwickelt, um dem in der Praxis vorhandenen Bedarf für eine starke Authentifizierung gerecht zu werden. Gleichzeitig wurde darauf geachtet, dass sie für die Endbenutzer leicht bedienbar ist und geringere Anwendungs- und Verwaltungskosten verursacht.

### Sichere und doch einfache Authentifizierung

**Entrust IdentityGuard bietet einen zweite Authentifizierungsfaktor.** Die vielleicht effektivste Art, eine Phishing-Attacke zu verhindern, ist, den Diebstahl der Online Identity des Benutzers aus der Ferne extrem zu erschweren. Diese Angriffe beruhen darauf, dass der Benutzer seinen Benutzernamen und sein Passwort über das Internet schickt und damit seine Identität einem Remote-Angreifer übermittelt. Mit der Entrust IdentityGuard Lösung hat es der Angreifer viel schwerer.

Der Diebstahl einer Online Identity kann durch den Einsatz eines zusätzlichen physischen Faktors beim Authentifizierungsprozess – etwas, das der Benutzer

zusätzlich zu dem hat, was der Benutzer lediglich weiß (sein Passwort), besser verhindert werden. Das verhindert, dass der Benutzer seine komplette Identität z. B. an eine gefälschte Website übermittelt. Auch wenn der Angreifer das Passwort des Benutzers erhält, hat er nicht den physischen Authentifizierungsfaktor und kann so nicht auf das Konto des Benutzers zugreifen.

Mit der Entrust IdentityGuard Lösung verwendet der Benutzer weiterhin seinen aktuellen Benutzernamen und sein aktuelles Passwort. Zusätzlich erhält er jedoch eine zweite, physische Form der Authentifizierung, die auf einer im Reihen-/Spaltenformat angeordneten Zeichenfolge, die auf einer Karte abgedruckt ist, basiert. Ein Beispiel zeigt die folgende Abbildung:

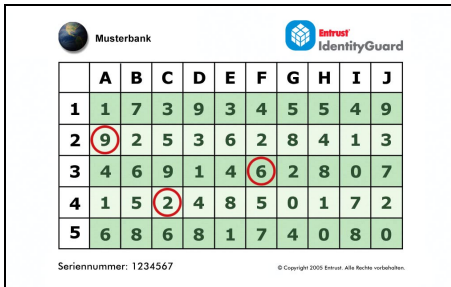
	A	B	C	D	E	F	G	H	I	J
1	1	7	3	9	3	4	5	5	4	9
2	9	2	5	3	6	2	8	4	1	3
3	4	6	9	1	4	6	2	8	0	7
4	1	5	2	4	8	5	0	1	7	2
5	6	8	6	8	1	7	4	0	8	0

Das tatsächliche Format der Karte ist sehr flexibel. Die Zelleninhalte können numerisch, alphanumerisch etc. sein, abhängig von den Anforderungen der jeweiligen Anwendung. Ebenso ist die tatsächliche Anzahl der Felder flexibel. Wichtig ist, dass jeder Benutzer eine zufällig generierte Zeichenfolge erhält, die er für die Authentifizierung verwenden wird.

Zur Authentifizierung verwendet der Benutzer seinen Benutzernamen und sein Passwort genauso wie bisher.

Zusätzlich erhält der Benutzer eine per Zufallsgenerator generierte Koordinatenabfrage, um nachzuweisen, dass er im Besitz der entsprechenden Karte ist.

Zum Beispiel, wenn der Benutzer zur Eingabe der Gitterkoordinaten A2, C4 und F3 aufgefordert wird:



	A	B	C	D	E	F	G	H	I	J
1	1	7	3	9	3	4	5	5	4	9
2	9	2	5	3	6	2	8	4	1	3
3	4	6	9	1	4	6	2	8	0	7
4	1	5	2	4	8	5	0	1	7	2
5	6	8	6	8	1	7	4	0	8	0

Ähnlich wie bei einer Bingokarte oder beim Nachschlagen eines Orts auf einer Landkarte gibt der Benutzer den Inhalt der Gitterzellen ein, die den abgefragten Koordinaten entsprechen. Bei diesem Beispiel würde der Benutzer die Werte der Gitterkoordinaten A2, C4 und F3 eingeben, also „9“, „2“ und „6“. Bei jeder nachfolgenden Anmeldung wird der Benutzer durch den Zufallsgenerator zur Eingabe einer anderen Kombination von Feldern aufgefordert.

So hat der Benutzer einen zweiten Authentifizierungsfaktor, der vor Phishing sicher ist. Selbst wenn ein Phishing-Angreifer das Vorhandensein dieser Methode herausfindet und einen Benutzer erfolgreich dazu verleitet, sich auf einer gefälschten Seite mit seinen Benutzerdaten anzumelden, wird der Angreifer nur eine Abfragekombination erfahren. Wenn der Angreifer diese Kombination anschließend auf der richtigen Internetseite verwenden will, würde er mit der Abfrage einer neuen zufällig generierten Kombination, deren Werte er nicht hat, konfrontiert werden. Auf einer 5 x 10 Karte wie in dem obigen Beispiel gibt es 19.600 verschiedene mögliche Kombinationen aus drei Koordinaten.

Dies steht in krassem Gegensatz zu der Methode der alleinigen Verwendung von Benutzernamen und Passwort, bei der eine einzige erfolgreiche Phishing-Attacke dazu führt, dass die Online Identity des Benutzers gestohlen wird.

**Entrust IdentityGuard bietet Sicherheit mit einer einfach anzuwendenden Methode.** Die von der Entrust IdentityGuard Lösung verwendete Methode macht sich Erfahrungen zunutze, die jeder schon gemacht hat. Die Benutzer werden diese Art der Authentifizierung von Spielen wie *Bingo* und *Schiffe Versenken* oder vom Nachschlagen von Orten auf einer Landkarte kennen. Dadurch, dass die Benutzer mit solchen Methoden bereits vertraut sind, bedarf es weniger Erklärungen für den Benutzer, um die Lösung anzuwenden.

Hinzu kommt, dass diese Methode auch hinsichtlich der äußeren Form des Entrust IdentityGuard Gitternetzes besser für den Einsatz in der Praxis geeignet ist. Das

Entrust IdentityGuard Gitternetz in Form einer Plastikkarte im Scheckkartenformat kommt den Authentifizierungsgewohnheiten eines modernen Benutzers besser entgegen: Die Plastikkarte kann man leicht mitnehmen und sie ist sehr robust. Während konventionelle Hardware-Token von der Technologie im Hardware-Gerät abhängig sind, das bisweilen fehlerhaft sein kann, wenn es physischem Missbrauch oder niedrigen Temperaturen ausgesetzt ist, sind Entrust IdentityGuard Gitterkarten haltbarer und können einem physischen Missbrauch besser standhalten.

## Abwehr komplexerer Identity Theft-Attacken

**Durch die Anwendung von Entrust IdentityGuard kann das Risiko, wiederholt Attacken durch Phishing oder Trojaner zum Opfer zu fallen, entscheidend gesenkt werden.** Es ist möglich, dass ein Benutzer nicht nur Angriffen in Form von einmaligen Phishing-Attacken, sondern komplexeren Angriffen zum Opfer fällt. Bei einer wiederholten Phishing-Attacke gibt der Benutzer wiederholt die Authentifizierungsinformationen auf einer gefälschten Website ein. Dies kann bei einem einzigen Login-Versuch geschehen, indem der Benutzer darauf hingewiesen wird, dass die Anmeldung nicht erfolgreich war und er aufgefordert wird, es noch einmal zu versuchen. Es kann aber auch über einen längeren Zeitraum durch wiederholte Phishing-E-Mails geschehen.

Ebenso wird bei einer Trojaner-Attacke auf dem Computer des Endbenutzers ein bössartiger Code installiert, der die Aktionen des Benutzers wie z. B. Tastaturanschläge scannt. Diese Informationen können lokal gespeichert werden und später über das Internet an den Angreifer übermittelt werden. Obwohl Firewalls und Virenschutzprogramme die Wahrscheinlichkeit, dass solche bössartige Software auf dem Computer eines Benutzers installiert wird, reduziert, wird es zwangsläufig eine bestimmte Anzahl von Benutzern geben, die nicht die neueste Virenschutzsoftware haben.

Wegen der großen Anzahl möglicher Abfragen und Antworten für jeden einzelnen Benutzer wird selbst bei Attacken, die mehrere Logins aufzeichnen, nur ein kleiner Teil des Authentifizierungsgitters übermittelt. Um weiterhin einen konsequenten und zuverlässigen Schutz zu gewährleisten, könnten den Benutzern regelmäßig neue Karten ausgestellt werden. Wenn eine Karte zum Beispiel ein Jahr im Einsatz war, könnte eine neue Karte generiert und an den Benutzer übersandt werden. Da bei dieser Methode keine spezielle Hardware an die Benutzer verschickt werden muss, ist es für Unternehmen sehr kostengünstig, die Karten regelmäßig zu ersetzen und neu auszustellen, um ein hohes Maß an Sicherheit zu bieten.

**Die flexiblen Kartenformate ermöglichen maßgeschneiderte Sicherheit zur Erfüllung der Kundenanforderungen.** Die Sicherheit des IdentityGuard Gitternetzes kann durch die Änderung seines Formats erhöht werden. Die größte Auswirkung auf die Sicherheit wird durch die Änderung der Anzahl der Gitterzellen erreicht. Durch die

Erhöhung der Anzahl der Reihen und/oder Spalten im Gitter nimmt die Sicherheit in ungefähr linearer Weise zu. Die Verdoppelung der Anzahl der Gitterzellen kann die Sicherheit zum Beispiel mindestens verdoppeln. Der andere das Kartenformat betreffende Faktor, der Einfluss auf die Sicherheit hat, ist die Entropie der einzelnen Zellen. Durch die Erhöhung der Anzahl der Werte in einer einzelnen Gitterzelle nimmt die Sicherheit zwar zu, jedoch in weit geringerem Maße als durch die Erhöhung der Anzahl der Zellen. Zum Beispiel nimmt die Entropie durch die Umstellung von einem einzigen alphanumerischen Zeichen auf eine zweistellige Zahl um das Dreifache zu. Die eigentliche Sicherheit erhöht sich dadurch jedoch nur um ca. 10%.

Für die meisten Einsätze auf eigenständigen Karten empfiehlt Entrust eine 5 x 10 Karte mit einem Zeichen pro Zelle. Dadurch ist ein gutes Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit gewährleistet. Die Entropie der Karte ist mit über  $10^{67}$  verschiedenen Gitternetzen hoch. Dadurch ist weitgehend sichergestellt, dass jede Karte einzigartig ist. Wie die Beispiele in diesem Artikel zeigen, ist ein Gitternetz aus 50 Zellen auch sehr gut lesbar. Das Ergebnis ist Sicherheit, die einen mehr als 10 Mal besseren Schutz vor Angriffen wie Phishing bietet, als Passwörter allein.<sup>6</sup> Für die meisten Kunden bedeutet das, dass sie jedes Gitter ein Jahr lang oder länger einsetzen und verwenden können.<sup>7</sup>

Ein weiterer Faktor, der bei der Anwendung berücksichtigt werden muss, ist, wie viele Zellen bei der Authentifizierungsabfrage abgefragt werden. Je kürzer die Abfrage, desto anfälliger ist sie für einen Brute-Force-Angriff, aber desto einfacher ist sie natürlich was die Benutzerfreundlichkeit angeht. Je länger die Abfrage, desto mehr Karteninformationen werden bei einem abgefangenen Login an den Angreifer übermittelt. Längere Abfragen erhöhen zwar den Schutz vor Brute-Force-Angriffen, sie sind aber auch weniger benutzerfreundlich. Entrust hat eine Vielzahl verschiedener Kombinationen entwickelt und herausgefunden, dass eine Abfragelänge von drei Zellen optimale Sicherheit und einen maximalen Schutz vor Brute-Force-Angriffen und abgefangenen Logins bietet.

Vielleicht noch wichtiger als diese detaillierten Sicherheitsüberlegungen ist die Tatsache, dass ein Unternehmen Angriffe möglicherweise einfach durch den Einsatz einer Lösung verhindern kann, die seine Website weniger angreifbar und damit für Angreifer weniger attraktiv macht.

<sup>6</sup> Vergleich mit der durchschnittlichen Anzahl von abgefangenen Logins, die erforderlich ist, um den Authentifizierungsfaktor herauszufinden.

<sup>7</sup> Die Sicherheitsexperten von Entrust können die Kunden dabei unterstützen, die für die spezifischen Kundenanforderungen am besten geeignete Konfiguration zu finden.

**Durch die Verwendung der zweistufigen Authentifizierungsmethode von Entrust IdentityGuard wird die Sicherheit weiter erhöht.** Die Entrust IdentityGuard Lösung unterstützt zusätzliche Sicherheitsstufen durch einen zweistufigen Authentifizierungsprozess, bei dem der Benutzer zuerst seinen Benutzernamen und sein Passwort für das normale Authentifizierungssystem wie unten abgebildet eingibt.

Daraufhin folgt eine zweite Authentifizierungsstufe, bei der der Benutzer auf der Grundlage der durch die Passwort-Anmeldung ermittelten Identität eine Abfrage folgender Sicherheitsmerkmale erhält:

- Abfrage eines gemeinsamen Geheimnisses (Shared Secret) wie z. B. der Seriennummer der Karte. Da diese nur dem Unternehmen bekannt ist, das das IdentityGuard Gitternetz ausgestellt hat, kann diese Methode vom Benutzer verwendet werden, um zu bestätigen, dass er tatsächlich mit dem richtigen Unternehmen kommuniziert. Falls diese Abfrage falsch oder gar nicht angezeigt wird, hat der Benutzer einen sofortigen visuellen Hinweis darauf, dass er sich möglicherweise auf einer gefälschten Seite befindet. In diesem Fall sollte er den Anmeldevorgang sofort abbrechen.
- Anzeige einer gesperrten Abfrage, die sich erst ändert, wenn die Daten richtig eingegeben wurden. Diese Abfrage ist mit dem jeweiligen Benutzerkonto auf der Grundlage der ersten Authentifizierungsstufe verbunden und ändert sich nicht, wenn der Dialog aktualisiert wird oder wenn die Antwort nicht korrekt eingegeben wird. Diese Methode verhindert, dass ein Angreifer die Abfragen so lange wiederholen kann, bis eine dabei ist, die ihm mehr zusagt. Sobald der Benutzer beide Authentifizierungsstufen erfolgreich abgeschlossen hat, wird die Abfrage mit Hilfe der Zufallsgeneratorfunktion von Entrusts FIPS 140-2 – zertifizierte Kryptographie – aktualisiert.

Diese unterstützt auch Anwendungen, bei denen der zweite Authentifizierungsfaktor Transaktionen vorbehalten ist, die als sensibler eingestuft werden. Eine zusätzliche Authentifizierung würde nur dann durchgeführt werden, wenn ein Benutzer auf diese Transaktionen zugreift. Dabei käme die oben beschriebene Abfrage- und Antwortfolge zum Einsatz.

### Multi-Channel-Authentifizierung

**Entrust IdentityGuard ist leicht erweiterbar, um weitere Authentifizierungsanforderungen zu erfüllen.**

In vielen Fällen werden die Transaktionen mit dem Benutzer nicht ausschließlich über das Internet abgewickelt. Andere Kommunikationsmittel sind z. B. das Telefon oder ein mobiles Gerät wie ein PDA (Personal Digital Assistant).

Die Entrust IdentityGuard Lösung kann für die verschiedenen Methoden der Kommunikation mit Kunden oder Geschäftspartnern genutzt werden. Die von Entrust IdentityGuard angewandte Abfrage- und Antwortmethode erfordert weder die Anzeige umfassender Informationsabfragen noch eine komplexe zeitbasierte Synchronisation. Ein Interactive Voice Response (IVR) System könnte z. B. einem Benutzer automatisch eine Koordinatenabfrage stellen, deren Antwort der Benutzer über die Tastatur seines Telefons eingeben würde.

Auf diese Weise könnte ein Unternehmen durch eine Investition allein in diese Technik bei allen verschiedenen Kommunikationsmitteln, durch die es mit seinen Benutzern kommuniziert, eine erhöhte Sicherheit bieten und dabei Kosten sparen und die Abläufe für die Benutzer vereinfachen.

### Einfache, kostengünstigere Anwendung

Unabhängig von der Stärke der Sicherheit kann keine Authentifizierungstechnik wirklich erfolgreich sein, wenn sie teuer und zu schwierig anzuwenden ist. Bisher hatten Unternehmen, die einen besseren Schutz vor Online Identity Theft erreichen wollten, nur die Wahl zwischen einer Art kryptographischem Token und einer komplizierten PIN/TAN-Methode. Entrust IdentityGuard ist eine Methode, die sowohl bei der Anschaffung als auch bei der Anwendung und laufenden Verwaltung kostengünstig ist.

### Anwendung

**Entrust IdentityGuard ist kostengünstig in der Herstellung und Anwendung.** Die Entrust IdentityGuard Lösung hängt nicht davon ab, auf welche Weise der Benutzer das Gitter erhält. Die Unternehmen können daher die für sie kostengünstigste und einfachste Methode wählen. Sie können das Gitternetz z. B. dem monatlichen Kontoauszug beifügen oder in Verbindung mit einer bereits eingesetzten Karte übermitteln.

**Musterbank**  
 Kontoauszug für:  
 Max Mustermann  
 Musterstraße 123  
 12345 Musterstadt

Kontonummer: 0982374987132  
 BLZ: 16-25-34  
 Kontoauszug: 13  
 Seite: 1 von 1  
 Dieser Kontoauszug deckt folgenden Zeitraum ab:  
 20.06.04-19.07.04

Datum	Beschreibung	Belastungen	Gutschriften	Saldo	
Saldoübertrag					2345,67
22.06.04	Kino	19,90		2325,77	
22.06.04	AB W/D 928347	60,00		2265,77	
25.06.04	CHQ#00013-1600193198		200,00	2465,77	
31.06.04	Geschäft XY	5,74		2260,03	

Reißen Sie das Papier entlang der Perforation ein, um Ihre Karte zu entnehmen.

A	B	C	D	E	F	G	H	I	J	
1	7	3	9	3	4	5	5	4	9	
2	9	2	5	3	6	2	8	4	1	3
3	4	6	9	1	4	6	2	8	0	7
4	1	5	2	4	8	5	0	1	7	2
5	6	8	6	8	1	7	4	0	8	0

Die Entrust IdentityGuard Lösung verwaltet den Inhalt der Gitterkarte für einen bestimmten Benutzer und liefert ihn in einem XML-Datenformat zur Integration in den gewünschten Weiterverarbeitungsprozess, z. B. die Herstellung einer Plastikkarte oder eines Schreibens wie oben abgebildet.

Im Gegensatz dazu müssen Hardware-Token zu deutlich höheren Kosten pro Benutzer gekauft und physisch verteilt werden. Aufgrund ihrer Form erfordert ihre Verteilung normalerweise einen eigenständigen Prozess, der wiederum mit erheblichen Organisations- und Verwaltungskosten verbunden ist.

Sogar Einmal-Passwortmethoden wie PIN/TAN-Lösungen können hohe Produktions- und Verteilungskosten verursachen. Normalerweise bestehen diese aus einer Serie von Einmal-Passwörtern, die jeweils ein Mal für einen Login benutzt werden können. Damit der Benutzer nicht den Überblick verliert, welche Einmal-Passwörter er bereits benutzt hat, sind die Passwörter oft unter einer schwarzen Schicht verborgen und müssen erst freigerubbelt werden, ähnlich wie bei Rubbellosen. So startet der Benutzer den Anmeldeprozess und rubbelt das nächste Passwort frei.

Da auf einem Blatt natürlich nur eine begrenzte Anzahl von Einmal-Passwörtern Platz hat, müsste diese Authentifizierungsmethode häufig wiederholt werden, möglicherweise innerhalb weniger Wochen. Die Rubbelform der Passwortliste zusammen mit der Häufigkeit der Verteilung erhöhen die Anwendungskosten deutlich.

**Entrust IdentityGuard unterstützt eine Vielzahl von Anwendungsfällen.** Entrust Identity Guard bietet für alle unterschiedlichen Methoden, die Unternehmen zur physischen

Verteilung des IdentityGuard Gitternetzes anwenden, eine Lösung und ermöglicht den Benutzern einen sofortigen Zugriff auf die Online-Dienste. Solche Anwendungsfälle könnten beispielsweise folgende sein:

- Der einfachste Fall ist, wenn die Benutzer zum selben Zeitpunkt, zu dem sie Benutzer von Entrust IdentityGuard werden, ihre Karte persönlich entgegennehmen können. Dadurch erhalten sie ihr Gitternetz und können es sofort verwenden.
- Benutzer, die ihr Gitternetz nicht sofort, sondern innerhalb eines relativ kurzen Zeitraums (z. B. innerhalb eines Tages) abholen, können den vorläufigen Passcode von Entrust IdentityGuard nutzen. Dieser Passcode kann für eine begrenzte Zeit oder für eine begrenzte Anzahl von Logins benutzt werden. Gleichgültig, ob er mündlich, telefonisch oder von einer interaktiven Website übermittelt wird, wird er bei der Authentifizierung einfach in die abgefragten Koordinatenfelder eingegeben. Da die Gültigkeit des Passcodes begrenzt ist, ist diese Methode mit geringem Risiko verbunden und ermöglicht den Benutzern den Zugang, bis sie ihr Gitternetz erhalten.
- In einigen Fällen ist es erforderlich, die Gitternetze physisch per Post zu verteilen und den Nutzern trotzdem einen sofortigen Zugang zu ermöglichen. In diesen Fällen kann eine vorläufige Bildschirmausgabe des Gitternetzes erstellt und über Anwendungen wie z. B. Adobe Acrobat gesendet werden. Diese würde verwendet, bis das physische Gitternetz per Post eintrifft. Um die Sicherheit bei diesem Prozess zu erhöhen, würde sich die Bildschirmausgabe von der physischen Ausgabe des Gitternetzes unterscheiden und hätte eine begrenzte Gültigkeitsdauer.
- Wenn ein sofortiger Zugang nicht erforderlich ist, können die Karten an die Benutzer verteilt werden, während sie weiterhin ihren aktuellen Benutzernamen und ihr aktuelles Passwort verwenden. Wenn sie die Karte erhalten, wird sie vom Benutzer telefonisch oder über eine interaktive Website freigeschaltet und für nachfolgende Authentifizierungen benutzt.

**Entrust IdentityGuard unterstützt stufenweisen Authentifizierungsprozess.** Eine starke Authentifizierung erfolgt oft in Stufen, entweder indem eine Stufe auf die andere folgt oder in Form eines optionalen zweiten Authentifizierungsfaktors. Die Entrust IdentityGuard Lösung unterstützt dies durch den bereits beschriebenen zweistufigen Authentifizierungsprozess, bei dem der Benutzer zuerst seinen Benutzernamen und sein Passwort für das normale Authentifizierungssystem eingibt. Nur bei Benutzern, die aktive Entrust IdentityGuard Benutzer sind, würde dieser zweite Bildschirm zur Entrust IdentityGuard Authentifizierung angezeigt werden.

## Niedrigere Kosten für die laufende Verwaltung

**Die Gesamtkosten können durch die gut durchdachte Verwaltung von Entrust IdentityGuard reduziert werden.**

Hohe Kosten für die laufende Verwaltung können oft die niedrigen Anschaffungs- und Anwendungskosten überschatten. Dies hängt weitgehend von drei wesentlichen Kostenfaktoren ab: Benutzerfreundlichkeit, Neuausstellung und Ersatzbeschaffung.

Wenn die Benutzer eine sichere Authentifizierung als schwierig zu bedienen empfinden, besteht die Gefahr, dass sich die Hotline-Anrufe häufen, was letztendlich die Supportkosten in die Höhe treibt. Die Gitternetz-Abfrage- und Antwortmethode von Entrust IdentityGuard benutzt eine sehr leicht zu verstehende Authentifizierungsmethode. Außerdem erhöht diese Methode dadurch, dass keine spezielle Hardware benötigt wird und man die Gitternetzkarte bequem überallhin mitnehmen kann, die Flexibilität enorm. Dies ist im Verbraucherbereich besonders wichtig.

Die Neuausstellung von Authentifizierungsgeräten kann erhebliche laufende Kosten verursachen. Im Gegensatz zu herkömmlichen Hardware-Token kann jedoch die Ausstellung eines neuen Entrust IdentityGuard Gitternetzes aufgrund seiner niedrigen Herstellungs- und Weiterverarbeitungskosten sehr kostengünstig sein. Sie ist auch einfacher als die PIN/TAN-Methode, bei der die Passwortliste des Benutzers ständig überwacht und rechtzeitig ausgetauscht werden muss, um sicherzustellen, dass dem Endbenutzer die Passwörter nicht ausgehen.

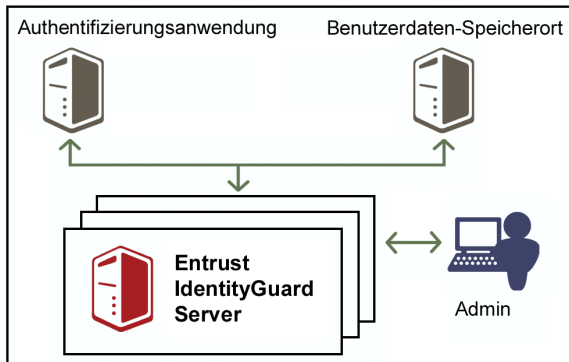
Es ist unvermeidbar, dass für den zweiten Authentifizierungsfaktor erforderliche Geräte bisweilen verloren gehen und ersetzt werden müssen. Es ist sehr wichtig, dass durch diese Situationen der Hotline kein erheblicher Aufwand entsteht oder dass der Benutzer für einen längeren Zeitraum keine Transaktionen mehr ausführen kann. Dies erhöht nicht nur die Kosten, sondern führt auch dazu, dass der Benutzer einen negativen Eindruck vom Unternehmen bekommt. Um dies zu verhindern, stellt die Entrust IdentityGuard Lösung die oben beschriebene Technik des vorläufigen Passcodes bereit. Dieser Passcode kann den Benutzern praktisch sofort zur Verfügung gestellt werden, wenn sie ihre Karte verloren oder verlegt haben. Ebenso kann für den Fall, dass es einige Zeit dauern wird, das Entrust IdentityGuard Gitternetz zu ersetzen, eine Bildschirmausgabe des Gitternetzes für eine höhere Sicherheit benutzt werden, bis die dauerhafte Ersatzkarte geliefert wird.

All diese Techniken tragen dazu bei, die von Entrust IdentityGuard bereitgestellte Sicherheit zu erhöhen und bieten eine kostengünstige Lösung für den Bedarf der Unternehmen für eine starke Authentifizierung.

## Architektur und Integration

Die Entrust IdentityGuard Lösung wurde so entwickelt, dass sie im Umfeld eines Unternehmens mit minimalen Auswirkungen auf die vorhandene Infrastruktur funktioniert. Dies gilt sowohl für die vorhandenen Authentifizierungs-

anwendungen als auch für die Benutzerdaten-Speicherorte. Die Lösung wurde auch für eine hohe Skalierbarkeit entwickelt und berücksichtigt die gegebenen Möglichkeiten wie Verfügbarkeit und Serviceniveaus, die in solchen Umgebungen wichtige Elemente sind.



### Unkomplizierte Integration

**Entrust IdentityGuard stellt eine Ergänzung der aktuellen Authentifizierungsanwendung eines Unternehmens dar.** Gleichgültig, ob es sich um eine selbst entwickelte Passwortanwendung oder um ein Produkt zur Internetzugangskontrolle eines Drittanbieters handelt, die Entrust IdentityGuard Lösung bietet eine Schnittstelle, durch die der zweite Authentifizierungsfaktor hinzugefügt wird. Praktisch alle gängigen Produkte zur Internetzugangskontrolle verfügen standardmäßig über eine Schnittstelle für genau diesen Zweck.

Die Authentifizierungsschnittstelle beruht entweder auf Java oder Web Services, um die Anforderungen verschiedener potenzieller Authentifizierungsanwendungen zu erfüllen. Die meisten Transaktionen konzentrieren sich auf die Authentifizierungsanwendung, wobei die vom Benutzer gegebene Antwort überprüft wird. Sobald diese bestätigt wird, würde der Entrust IdentityGuard Server das Ergebnis liefern.

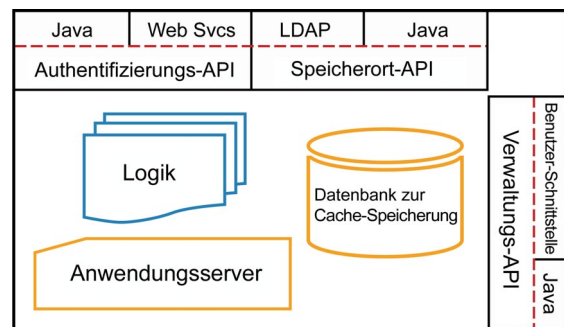
Zusätzlich kann diese Schnittstelle dazu benutzt werden, die in der Abfrage tatsächlich zu verwendenden Koordinaten zu liefern. Dies verringert die Auswirkungen auf die aktuelle Authentifizierungsanwendung noch mehr. Es trägt auch dazu bei, das Risiko eines Angriffs zu senken, wenn ein kleiner Teil des Gitternetzes bekannt ist. Wie oben beschrieben, benutzen zweistufige Authentifizierungsmethoden dieselbe Abfrage für einen Benutzer, bis er sich erfolgreich eingeloggt hat. Dadurch wird verhindert, dass der Angreifer einfach so lange die Aktualisieren-Schaltfläche seines Browsers anklickt, bis eine Abfrage angezeigt wird, die mit den Feldern, die der Angreifer möglicherweise bereits kennt, übereinstimmt. Entrust IdentityGuard verfolgt laufend die aktuelle Abfrage für jeden Benutzer und stellt sie der Anwendung auf Anfrage zur Verfügung.

**Vergleichbar mit der Schnittstelle zu der Authentifizierungsanwendung nutzt Entrust IdentityGuard den vorhandenen Speicherort des Kunden zur Speicherung der Benutzerdaten.** Dieser Speicherort wird zum Speichern und Abrufen der Kartendaten der einzelnen Benutzer verwendet. Wird eine Karte für einen bestimmten Benutzer generiert, wird sie in verschlüsselter Form im Speicherort abgelegt. Bei der Authentifizierung eines Benutzers wird sie vom Speicherort abgerufen. Diese Schnittstelle unterstützt LDAP, JDBC und kundendefinierte API.

Schließlich wird eine Remote-Access-Webschnittstelle zur Verfügung gestellt, um die verschiedenen Benutzer- und Kartenverwaltungsfunktionen zu nutzen. Dazu gehört die Möglichkeit, neue Karten zu erstellen, vorläufige Passcodes zu vergeben und den Benutzer- und Kartenstatus zu aktualisieren. Verwaltungsfunktionen stehen auch per API zur Verfügung, sodass sie für Benutzeridentitätsverwaltungs- und Beschaffungssysteme genutzt werden können.

### Stabile, flexible Architektur

**Entrust IdentityGuard wurde entwickelt, um die Anforderungen an die Skalierbarkeit verbraucherorientierter Anwendungen mit hohem Transaktionsvolumen zu erfüllen.** Deshalb ist diese Lösung so konstruiert, dass mehrere Server gleichzeitig in einer Load-Balanced-Umgebung eingesetzt werden können. Dies ermöglicht einen erhöhten Durchsatz durch das Hinzufügen zusätzlicher Server. Außerdem steht eine eingebettete Datenbank zur Verfügung, um die Benutzer- und Karteninformationen im Cache-Speicher abzulegen, um die Transaktionen zu beschleunigen.



Die Entrust IdentityGuard Lösung basiert auf einem serverbasierten Softwareprodukt, das in der vorhandenen Infrastruktur des Unternehmens installiert wird. Sie ist in Java geschrieben und läuft auf dem Betriebssystem Linux. Sicherheitsoperationen wie das Generieren, Verschlüsseln und Entschlüsseln von Karteninhalten werden mit Entrusts Verschlüsselungssoftware FIPS 140-2, die nach Common Criteria zertifiziert ist, durchgeführt. Diese Methode gewährleistet, dass der Inhalt jeder Karte sicher ist. Außerdem wird das Risiko reduziert, dass ein Mitarbeiter mit böswilligen Absichten Zugang zu den Karteninformationen im Speicher erhält.

Schließlich wird wie bei allen Entrust Produkten größte Sorgfalt auf die Softwareentwicklung, Qualitätssicherung und Sicherheit gelegt, um die höchsten und anspruchsvollsten Kundenanforderungen zu erfüllen. Außerdem stehen für die Entrust IdentityGuard Lösung Entrusts weltweite Service- und Supportdienste an 365 Tagen im Jahr rund um die Uhr zur Verfügung.

## Zusammenfassung

Mit der weiteren Zunahme des Online Identity Theft müssen die Unternehmen das Risiko mit einer stärkeren Form der Authentifizierung aktiv senken. Diese Methode muss leicht zu bedienen sowie ihre Anschaffung und Anwendung kostengünstig sein. Entrust IdentityGuard deckt diesen Bedarf durch eine einfache, innovative und

kostengünstige Lösung zur Erhöhung der Sicherheit und zum Schutz vor Angriffen.

Unternehmen, die Maßnahmen gegen Identity Theft ergreifen, haben die Möglichkeit, ihre durch die Angriffe entstehenden Verluste zu reduzieren sowie das Vertrauen ihrer Benutzer zu gewinnen, um die Akzeptanz der Online-Dienste zu erhöhen.

Entrust IdentityGuard ist Teil der Entrust Secure Identity Management Lösung und ist in die anderen Elemente der Lösung für eine starke Authentifizierung und Zugangskontrolle eingebunden. Weitere Informationen darüber, wie Sie mit Entrust IdentityGuard Schäden durch Identity Theft und Phishing minimieren können, erhalten Sie unter: <http://www.entrust.com/IdentityGuard/>.

## Über Entrust

Entrust, Inc. [NASDAQ: ENTU] ist ein weltweit führender Anbieter im Bereich der Sicherung digitaler Identitäten und Informationen. Über 1.400 Unternehmen und staatliche Behörden in mehr als 50 Ländern vertrauen auf Entrust Lösungen, um die digitalen Daten ihrer Bürger, Kunden, Mitarbeiter und Geschäftspartner zu schützen. Unsere erprobten Software-Anwendungen und Dienstleistungen unterstützen unsere Kunden dabei, die Anforderungen von Aufsichtsbehörden und Unternehmen zu erfüllen und ermöglichen ihnen, durch die Bewältigung von Sicherheitsrisiken wie Identity Theft und Phishing-E-Mails einen Wettbewerbsvorteil zu ziehen. Weitere Informationen darüber, wie Sie mit Entrust Ihre digitalen Daten schützen können, erhalten Sie unter: [www.entrust.com](http://www.entrust.com).