

Der elektronische Banküberfall ist alltäglich geworden!

Der elektronische Banküberfall ist alltäglich geworden. Dabei werden oft Schwachstellen ausgenutzt, die sich beim Anwender und nicht auf der Onlinebanking-Plattform befinden.

Wettlauf mit dem Angreifer

Jede Welle von Angreifern auf eine Online-Banking-Plattform brachte eine schnelle Reaktion der Hersteller mit sich und dadurch eine stetige Verbesserung der Plattformen. Mit dem Resultat, dass die bankseitigen Systeme und Anwendungen heute praktisch keine Schwachstellen mehr aufweisen. Deshalb ist inzwischen der Benutzer zum Ziel der Angreifer geworden. Denn dessen Systeme befinden sich ausserhalb des Einflussbereichs der Banken und sie sind trotz Schutzprogrammen oft überfor-

dert. Hinzu kommt, dass die Angreifer mittlerweile sehr professionell und gut organisiert vorgehen.

Wie sollen die Banken reagieren?

Die Onlinebanking-Plattformen können dahin ausgebaut werden, dass der Zugang zur Anwendung und die anschliessenden Transaktionen analysiert werden und bei Verdacht auf Missbrauch eine vordefinierte Reaktion eingeleitet wird. Dabei ist denkbar, den Kunden telefonisch zu kontaktieren, die laufende Onlinebanking-Sitzung sofort zu unterbrechen oder die Vertragsnummer zu sperren.

Schaffen sie sich mit uns Transparenz gegenüber Angriffen von aussen

Totale Sicherheit gibt es nicht. Doch lässt sich mit dem

Fortsetzung nächste Seite.

Wettbewerb

Wir planen weiter als nur bis zur EURO2008

Wie heisst die «Queen of Pop» welche am 30. August 2008 mit Ihrer «Sticky & Sweet»-Tour in die Schweiz kommt?

Machen Sie mit und gewinnen Sie mit etwas Glück 3x2 Tickets (Sitzplätze, gedeckte Tribüne) für das Konzert auf dem Militärflugplatz in Dübendorf.

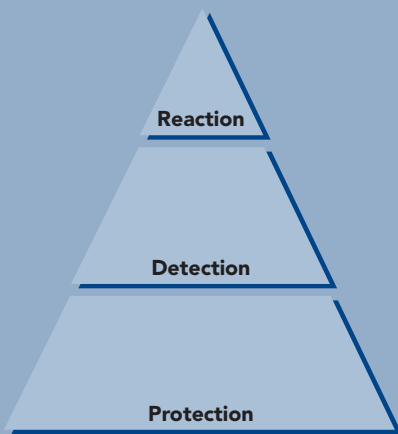
Wie machen Sie mit?

Wenn Sie den Namen der Künstlerin wissen, senden Sie uns eine E-Mail und setzen als Name vor dem «@»-Zeichen den der Künstlerin ein:@terreactive.ch. Vergessen Sie nicht Ihren Namen sowie die Geschäfts- und Privat-Adresse anzugeben.

Der Wettbewerb wird nur in unserem Newsletter 1/2008 veröffentlicht. Teilnahmeberechtigt sind nur die Empfänger des Newsletter-Mails.

Teilnahmeschluss: 31. Juli 2008

Die Auslosung findet unter Ausschluss von Dritten am 4. August 2008 im Firmensitz von terreActive AG statt. Die Gewinner werden schriftlich benachrichtigt und nicht veröffentlicht. Die Tickets werden an die Privat-Adresse geschickt. Diese wird nicht gespeichert und auch nicht für Marketing-Zwecke verwendet. Es erfolgt keine Barauszahlung der Preise. Der Rechtsweg ist ausgeschlossen.



Einsatz von IT-Sicherheits-Monitoring der neuesten Technologie und steter Überwachung die bestmögliche Schadensbegrenzung erzielen. Im Zusammenhang mit einer ausgeglichenen Sicherheitsarchitektur (siehe Grafik)

hat sich der Begriff des Security Event Management (SEM) als Schlüsseltechnologie im Detection-Bereich etabliert. Dabei werden durch die Korrelation vorhandener Log-Informationen der Systeme und Anwendungen Sicherheitsevents modelliert und Unregelmässigkeiten beim Betrieb von Sicherheitsinfrastrukturen automatisch erkannt. Konkret ist die Analyse des Zugangs zur Anwendung und den Transaktionen gemeint.

Wir wissen wovon wir sprechen!

Die SEM-Lösung tacLOG wurde für den Einsatz im E-Business- und Onlinebanking-Umfeld entwickelt und deckt daher diese Bedürfnisse optimal ab.

Da wir als Managed Security-Anbieter schon früh mit solchen Sicherheitsvorfällen konfrontiert wurden, haben wir unsere langjährige Erfahrung in diese rein Schweizerische Lösung einfließen lassen. Seit 2001 auf dem Markt erfreut sich tacLOG einer ständig wach-

senden Beliebtheit. Mit über 25 erfolgreichen Projekten und mehr als 100 Appliances im 7 x 24 h-Einsatz zählt tacLOG zu den führenden Lösungen im Schweizer Markt. Unsere Kunden kommen nicht nur aus dem Finanzmarkt und der Verwaltung, sondern sind immer mehr auch in der Industrie, Telecom oder dem Gesundheitswesen zu finden.

Stete Sensibilisierung der Bankinstitute

Dieses aktuelle Thema, welches die E-Banking-Welt in nächster Zeit noch in Atem halten und fordern wird, haben wir den Lesern der Fachzeitschrift Netzguide in der letzten Ausgabe näher gebracht. Ziel von uns ist es, unsere Kunden als kompetenter IT-Sicherheits-Partner in allen Belangen der IT-Sicherheit zu unterstützen.

Dieser Newsletter-Beitrag ist ein stellenweiser Auszug aus dem Fachartikel. Den ganzen Artikel finden sie auf unserer Homepage.

Weitere Informationen:

<http://www.terreactive.ch/newsletter>

Totemo – unser E-Mail-Verschlüsselungs-Partner

totemo ag

Als wir von einem Kunden den Auftrag erhielten, eine E-Mail-Verschlüsselungslösung zu evaluieren,

war das Thema noch relativ neu. Unsere Berater haben sich den Markt genau angesehen und verschiedene Lösungen getestet. Am Schluss gewann etwas überraschend – die meisten Anbieter kommen aus den USA – eine Schweizer Lösung unser hartes Auswahlverfahren.

Die Firma Totemo AG, unweit von Zürich am rechten Seeufer gelegen, brachte mit ihrer Lösung «TrustMail» alles mit, was wir als IT-Sicherheitsexperten forderten, und sie konnte zusätzlich durch ihre lokale Kompetenz überzeugen.

Die lange Referenzliste von Totemo zeigt, dass ihr Produkt heute kein Geheimtipp unter IT-Sicherheitsexperten mehr ist, sondern eine breite Akzeptanz im Markt genießt.

Auch wir sind überzeugt, dass der Markt noch stark wachsen und E-Mail-Verschlüsselung bald zum Standard in vielen Unternehmen gehören wird. Unsere enge Zusammenarbeit mit Totemo wird unseren Kunden sicher helfen, E-Mail-Verschlüsselung schnell und erfolgreich einführen zu können.

Weitere Informationen:

<http://www.totemo.ch>

<http://www.terreactive.ch/newsletter>

Zentrale Monitoring-Lösung im Einsatz bei Dienstleistungszentrum für Finanzinstitute

Als Dienstleistungszentrum für Finanzinstitute konzentriert sich die sourcag auf die Abwicklung des Wertschriftengeschäfts, des Zahlungsverkehrs sowie auf das Outsourcing von Informatik-Dienstleistungen für Kunden. Zu den Aufgaben der Informatik sourcag gehören unter anderem die permanente Betreuung und Überwachung der ihr anvertrauten Informatik-Systeme. Die betreute Systemlandschaft umfasst unterschiedlichste Anwendungsserver, Netzwerk-Komponenten und Schnittstellen (Firewalls). Im Operating Center des Service Desk der Informatik laufen die relevanten Informationen von über 1'000 Objekten der Kunden zusammen. Die sourcag stellt sicher, dass eine lückenlose Überwachung und Intervention der IT-Systeme jederzeit gewährleistet ist.

Die zunehmende Komplexität und die steigende Anzahl der überwachten Objekte waren wichtige Impulsgeber für die Suche nach einem Ersatz der teilweise selbst entwickelten Monitoring-Lösung. Insbesondere beim SLA-Reporting war die bestehende Lösung aus Gründen der Performance an Grenzen gestossen.

Monitoring-Lösung von terreActive

Die erwähnte Ausgangslage war die Basis für die von sourcag durchgeführte Evaluation. Die Kombination von aktivem (tacMON) und passivem (tacLOG) Monitoring war für den Entscheid zu Gunsten von terreActive wichtig. Gerade die zentrale Logdaten-Analyse durch tacLOG bringt den Informatikern bei sourcag weitere wertvolle Informationen zur effektiven Behebung von Störungen.

Realisierung

Bei der Implementierung haben sourcag und terreActive sehr eng zusammengearbeitet. Die notwendigen Prozesse wurden genau definiert und konzeptionell vorbereitet. Der Parallel-Betrieb zur bestehenden Lösung stellte in einer ersten Phase die vereinbarten Dienstleistungen sicher. Der Wechsel vom alten System zu unserer Lösung erfolgte anschliessend fließend.

«Wir haben uns für die Lösung von terreActive entschieden, weil sie unsere Ansprüche am besten erfüllt und wir unseren Kunden so ein umfassendes Monitoring in hoher Qualität anbieten können.»



Timo Anthes
Business Architect IT
sourcag AG

Vorteile aus Sicht des Kunden

sourcag sieht folgende wichtige Vorteile:

- Umfassendes Monitoring mit hoher Qualität
- Systeminformationen stehen jederzeit Online zur Verfügung
- Frühzeitige Erkennung von Engpässen bei Systemressourcen
- Reduzierte Ausfallzeiten dank proaktivem Fehlermanagement
- Erheblicher Zeitgewinn beim SLA-Reporting
- Tiefere Kosten dank einfachem Lizenzierungsmodell

Dieser Newsletter-Beitrag ist ein stellenweiser Auszug aus der Success Story «sourcag». Den ganzen Artikel finden sie auf unserer Homepage.

Weitere Informationen:

<http://www.sourcag.ch>

<http://www.terreactive.ch/newsletter>

Neue Angebote

IT-Security Experts

In den letzten Monaten haben wir immer mehr von Ressourcen-Engpässen bei unseren Kunden erfahren. Das hat uns dazu bewogen, unsere eigenen Experten punktuell zur Verfügung zu stellen. Dies soll nicht ein typisches «Body-Leasing» sein, sondern über periodische Einsätze mit klaren Zielvorgaben geschehen.

Unsere Kunden erhalten drei wichtige Vorteile:

1. Unsere Experten sind immer noch stark bei terreActive integriert und erweitern über Projekte und Trainings ständig ihr Wissen, was wiederum dem Kunden zugute kommt.
2. Durch die klaren Zielvorgaben entsteht keine zusätzliche Abhängigkeit von einzelnen Mitarbeitern

und wir können, falls nötig, schnell einen Ersatz für den Experten bereitstellen.

3. Die periodischen Einsätze zusammen mit den klaren Zielvorgaben schaffen Transparenz und sparen Kosten gegenüber dem typischen «Body-Leasing».

Interessiert?

Senden Sie uns Ihre Anfrage an marketing@terreactive.ch oder kontaktieren Sie Herrn Rolf Hefti.

Compliance Reporting

Compliance Reporting wird für viele Unternehmen immer wichtiger. Nicht nur die Banken und wie bei SOX die in den USA börsenkotierten Unternehmen sind betroffen. Mit neuen Vorgaben wie dem PCI-DSS (Payment Card Industry-Data Security Standard) kann es auch Gruppen von Unternehmen (E-Shops, Airlines, Grossverteiler etc.) treffen, die beispielsweise grosse Mengen von Kreditkarten-Transaktionen verarbeiten oder Kreditkarten herstellen. Da werden IT-Sicherheits-Überprüfungen und die Überwachung der IT-Sicherheit auf einmal zur Pflicht. Gerade für Unternehmen welche sich bis anhin weniger stark mit IT-Sicherheit auseinander setzen mussten, bedeutet es eine grosse Herausforderung.

terreActive Mitglied bei PCI-SVA



Wir sind seit letzten Herbst Mitglied der PCI Security Vendor Alliance (SVA). Dies bietet uns und unseren Kunden die Möglichkeit am Puls des Geschehens dabei zu sein und stets über die wichtigsten Neuerungen und Standards informiert zu bleiben.

terreActive als PCI-Partner

Für neue Kunden liegen wir mit unserer SIEM-Lösung gerade richtig und können mit wenig Aufwand schnell erste Resultate liefern, welche auch vor einem Audit bestehen. Da wir selbst Audits durchführen – bei grossen und kleinen Unternehmen verschiedener Branchen – wissen wir worauf es ankommt.

Unsere bestehenden SIEM-Kunden haben immer weiterführende Compliance Reporting-Bedürfnisse. Das hat uns veranlasst, diesen Punkt in die Release-Planung aufzunehmen und mit den nächsten Versionen unserer SIEM-Lösung (tacLOG) stetig weiter zu entwickeln.

Weitere Informationen:

PCI DSS Homepage
<http://www.pcisecuritystandards.org>

PCI SVA-Homepage
<http://www.pcialliance.org>

<http://www.terreactive.ch/newsletter>

Schulungen bei terreActive

Im Herbst 2008 bieten wir erstmals Schulungen zu unseren Produkten tacLOG und tacMON an. Bitte reservieren Sie sich die Daten oder melden Sie sich gleich an unter:

<http://www.terreActive.ch/training>

Thema	Details	Datum, Zeit, Kosten
Einführung ins Thema SEM/SIEM (Evaluation einer SIEM-Lösung) • Zielpublikum: CIOs, IT-Security Officers, IT-Betriebsleiter	<ul style="list-style-type: none">• Evaluation einer SIEM-Lösung• Vorgehen bei Einführung• Log-Konzept• Umsetzung Konzept anhand von Beispiel• Demo des SEM-Tools tacLOG (tacMON)	<ul style="list-style-type: none">• 4. September 2008• Dauer: 4 h• Kosten: CHF 750
Einführung tacLOG SIEM-Lösung • Zielpublikum: Anwender tacLOG	<ul style="list-style-type: none">• Konzept und Einsatzgebiet• Übersicht Funktionen• Bedienung der Benutzeroberfläche• Diverse Themen: Log-Suche, kombinierte Darstellung, Zusammenhang Events – Logdaten etc.• Praktische Übungen auf Demo-Umgebung	<ul style="list-style-type: none">• 10. September 2008• Dauer: 3 h• Kosten: CHF 500
Administration tacLOG • Zielpublikum: Administratoren	<ul style="list-style-type: none">• Aufgaben des Administrators aufzeigen• Log-Daten analysieren• Events und Alerts erstellen• Erstellen von eigenen grafischen Auswertungen• Erstellen von Reports• Erlernte Funktionen anhand von Beispielen vertiefen	<ul style="list-style-type: none">• 16. September 2008• Dauer: 6 h• Kosten: CHF 1'250
Administration tacMON • Zielpublikum: Administratoren	<ul style="list-style-type: none">• Aufgaben des Administrators aufzeigen• Vorgehen und Konzepte• Erstellen von Projekten• Integration von Objekten• Festlegen von Schwellwerten und Alarmierung• Erstellen von Reports	<ul style="list-style-type: none">• 2. Oktober 2008• Dauer: 4 h• Kosten: CHF 750

Produkte News

Aktuelle Informationen zu unseren Produkten / Partnerprodukten:

Produkt	Details
SEM/SIEM-Lösung tacLOG Aktuelle Version: 2.10	<ul style="list-style-type: none">• Über 500'000 Dateien können verwaltet und durchsucht werden• Stark verbesserte Performanz der Benutzeroberfläche (GUI)• Direkte Konfiguration von «Views» im GUI• Vorauswahl von «View» und «Layout» in Kombination mit Filtern für die Einstiegsseite• Neue syslog-ng Version 2.0• Web-Links im Text der Logzeilen machen die Bedienung effizienter• Verschleiern von bestimmten Textstellen bei der Anzeige der Logzeilen• Direkter Zugriff, dank Filterkriterien und View-Auswahl gemeinsam als Lesezeichen («Bookmark») abspeichern
tacASG Aktuelle Version: 3.1	<ul style="list-style-type: none">• Durchsatz über 20'000 Mails pro Stunde• Quarantäne-GUI für die SPAM-Verwaltung• E-Mail-Rapport über Viren- und SPAM-Mails an individuelle Nutzer• AntiVirus-Modul mit ClamAV (Open Source) oder Kaspersky• Integration in tacMON: Grafische Auswertung der wichtigen Parameter• Integration in tacLOG: Anzeige der relevanten Logzeilen pro E-Mail• SPAM-Erkennungsrate: > 99%, bleibt in Kombination mit MSS-Service permanent auf diesem hohen Niveau
tacMON Aktuelle Version: 2.18	<ul style="list-style-type: none">• Verbessertes Event-Handling durch neue GUI-Funktionen wie verschachtelte Gruppierung• Alarmierung und Warnung pro Scan konfigurierbar• Authentifizierung der tacMON-Nutzer über LDAP• Automatischer Abgleich der tacMON-Nutzer mit tacLOG• Schwellwerte für relative SNMP-Werte• Erweiterter SLA-Scanner für SNMP- und APPS-Scan-Resultate
Totemo Trustmail Aktuelle Version: 3.1	<ul style="list-style-type: none">• Secure Messaging Gateway Lösung• Einfache Integration in die bestehende E-Mail-Infrastruktur• Keine Anpassungen an den Clients notwendig• Zentrale Umsetzung der Security Policy
Visonys Airlock Aktuelle Version: 4.1	<ul style="list-style-type: none">• Die Schweizer Web Application Firewall• Multi-Level Filter Engine• Access Control, mit Single-Sign-On-Funktionen• Application Delivery (Load Balancing auf Anwendungsebene)• Monitoring und Reporting auf Basis von tacLOG (Analyse, Compliance)

Neue Mitarbeiter

Daniel Tejido
Presales Engineer



Ausbildung:
IT Services Engineer HF/TS

Hobbies:
Klettern, Technologie



Felipe Kaufmann
IT Security Engineer



Ausbildung: Wirtschafts-
informatiker Uni Fribourg

Hobbies: Hochtouren, Musik,
Downhill Skateboarden etc.



NEXT

Folgende Events und Veröffentlichungen sind geplant:

- **Security Breakfast Bern, 26. Juni 2008**
Themen: E-Government, IT-Sicherheit, Compliance, Open Source
- **Success Story, Juni/Juli 2008**
mit Basler Kantonalbank
- **Newsletter 2|2008, August/September 2008**
- **Teilnahme Security Zone, 24./25. September 2008**
- **Teilnahme WinLink-Fachtagung, 2. September 2008**
- **Security Breakfast Zürich, 4. November 2008**
Themen: Details im nächsten Newsletter

Abonnemente

Dieser Newsletter erscheint exklusiv auf dem Internet und kann durch Angabe der E-Mail Adresse kostenlos abonniert werden. Er richtet sich in erster Linie an Kunden, Partner und der Firma terreActive nahe stehende Personen, welche sich über die Geschehnisse rund um terreActive informieren möchten.

Die – auch auszugsweise – Reproduktion, Übersetzung sowie sonstige Verwendung der Inhalte des Newsletters ist nur nach ausdrücklicher Genehmigung durch terreActive AG gestattet.