

## Schützen Sie sich erfolgreich vor Computerkriminalität

**terreActive baut das Managed Security Service Angebot weiter aus. Der neue IT-Sicherheits-Management Service hilft auch kleineren Unternehmen ohne eigenes IT-Sicherheitsteam, sich effizient und erfolgreich vor Computerkriminalität (Cybercrime) zu schützen.**

Die IT-Sicherheit kennt trotz der aktuellen Wirtschaftslage keine Krise. Zur Zeit wachsen die Angriffe auf Unternehmen und Privatpersonen im zweistelligen Prozentbereich. Die Menge des Schadcode explodiert sogar und man geht von über 1.7 Billionen Varianten im Jahr 2008 aus. Dies führt bei den Herstellern von Schutzsoftware zu ständigem Druck, mit dem sich schnell verändernden Schadcode mithalten zu können. Dies gelingt immer weniger und führt dazu, dass auch die aktuellsten Anti-Virus Lösungen den neusten Schadcode nicht mehr erkennen können.

terreActive hat diese Bedrohung schon vor Jahren vorausgesehen und fokussierte sich daher vermehrt auf die sogenannte «Detection» oder Sicherheitsüberwachung. Dabei geht es darum, ungewöhnliches Verhalten der IT-Infrastruktur zu erkennen. Beispielsweise muss erkannt werden, wenn eine Workstation versucht, über Wege in das Internet zu gelangen, welche nicht durch die normale Nutzung verursacht werden.

Dabei muss natürlich bekannt sein, was die normale Nutzung ist und wann von einem ungewöhnlichen Verhalten gesprochen werden kann. Die Beantwortung dieser einfachen Fragen ist in der Praxis alles andere als trivial und setzt sehr gute Kenntnisse der gesamten IT-Infrastruktur und der aktuellen Bedrohungslage voraus.

In der Realität sind heute viele Unternehmen nicht in der Lage, diese Fragen selber zu beantworten. Entweder fehlen die eigenen Ressourcen oder sie werden von externen Anbietern bezogen (Outsourcing). Meist sind dann zwar komplexe SLA-Verträge vorhanden, die IT-Sicherheit wird darin aber nur selten behandelt.

terreActive hat das Bedürfnis vieler Unternehmen nach einem unabhängigen und spezialisierten IT-Sicherheits-Manager erkannt.

Deshalb baut sie ihr Managed Security Service Angebot weiter aus und bietet neu neben den Operation und Security Alarming Services auch IT-Sicherheits-Management an. Dadurch kann der Grossteil der IT-Sicherheit an terreActive ausgelagert werden, jedoch ohne die Kontrolle darüber zu verlieren.

(Fortsetzung Seite 2)

## «Samichlaus du liebe Ma ... »

**Wir suchen die besten selbstgedichteten Samichlaus-Versli. Texten Sie zusammen mit Ihrem Team/ Ihren Arbeitskollegen einen Vers und mit etwas Glück kommt am 4. Dezember der terreActive-Samichlaus bei Ihnen zu Besuch.**

### So nehmen Sie teil:

Senden Sie Ihren Vers unter Angabe der Anzahl IT-Mitarbeiter und der genauen Anschrift Ihrer Firma an [samichlaus@terreactive.ch](mailto:samichlaus@terreactive.ch)

**Teilnahmeschluss: 27. November 2009**

Unsere Mitarbeiter werden die Verse bewerten. Die drei mit den meisten Stimmen bekommen einen Überraschungs-Besuch vom Samichlaus.



Alle Verse werden auf unserer Homepage publiziert.

**Viel Spass beim Dichten!**

Das heutige Basisangebot sind die als Baukastensystem erhältlichen Dienstleistungen zum Betrieb der IT-Infrastruktur. Darunter fallen alle Aufgaben, welche für den Betrieb von Sicherheitskomponenten wie Firewalls oder Proxies notwendig sind.



Mit dem Security Alarming Service übernimmt terreActive die Sicherheitsüberwachung eines Teils oder der gesamten IT-Infrastruktur. Wir sammeln alle relevanten Informationen, interpretieren die Daten und reagieren entsprechend den im Voraus definierten Handlungsanweisungen.



Der neueste Bereich von Services wendet sich an mittlere Unternehmen aus dem Finanzbereich, Versicherungs- und Gesundheitswesen, Government und der Industrie, welche nicht die Möglichkeiten haben, eigene IT-Sicherheitsteams zu beschäftigen. terreActive kann in diesen Fällen das gesamte IT-Sicherheits-Management übernehmen und direkt dem IT-Leiter oder Sicherheitsverantwortlichen rapportieren. Dabei helfen dem Kunden spezielle Tools und Reports, um terreActive selber zu kontrollieren und eine echte Gewaltentrennung zu erreichen.



## Die Firma terreActive. Managed Security Services.



IT-Sicherheits-Management



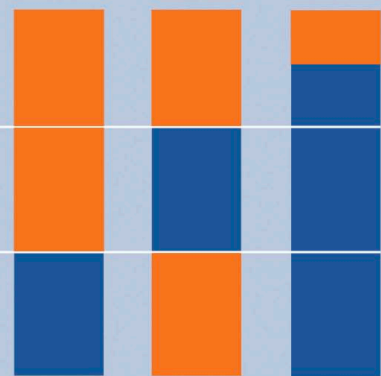
Security Alarming  
(Reporting, Compliance)



Operation / Support



Variante A      Variante B      Variante C



orange durch Kunde  
blue durch terreActive

Mit über 50 Betriebskunden gehört terreActive zu den führenden Anbietern im Schweizer Markt. Prüfen Sie bei der nächsten Einführung einer neuen IT-Sicherheitskomponente, in welchem Ausmass Sie den Betrieb selber machen wollen und lassen Sie sich in einem kostenlosen Beratungsgespräch die möglichen Einsparungen und Entlastungen durch unser Managed Security Service Angebot aufzeigen.

**Weitere Informationen:**

<http://www.terreActive.ch>

# Kunden-News

## 3 Erfolgsgeschichten mit langjähriger Zusammenarbeit



### Bedürfnisse sind wichtig

«Mit den Managed Security Services, die wir – genau auf unsere Bedürfnisse zugeschnitten – bei terreActive beziehen, erreichen wir einen sehr hohen Sicherheitsstandard bei gleichzeitig grosser Flexibilität, um auf neue Anforderungen zu reagieren.» Adrian Gloor, Leiter Organisation und Informatik, Stadt Aarau

#### Projekt:

Managed Security Services

Die wichtigsten Vorteile in unserer Zusammenarbeit sieht Herr Gloor wie folgt:

- Optimale Sicherheit durch Managed Security Services
- Kombination von verschiedenen Elementen erhöht Sicherheit
- IT-Infrastruktur wird rund um die Uhr überwacht
- Minimaler Aufwand für die Administration dank MSS
- Direkte Hotline für Anfragen jeder Art



### Nicht ohne tacLOG

«Seit wir tacLOG bei uns im Einsatz haben, kann ich mir nicht mehr vorstellen, jemals wieder darauf verzichten. Das zentrale Log-Management von terreActive entspricht genau unseren Bedürfnissen und erleichtert unsere Aufgabe enorm.» Andreas Hüppi, Network-Security, Kanton Aargau

#### Projekt:

Log-Management

Die wichtigsten Vorteile in unserer Zusammenarbeit sieht Herr Hüppi wie folgt:

- Zentrale Verwaltung von Logdateien
- Senkung des Aufwands für die Systemadministration
- Erhöhung der Netzwerksicherheit
- Bedürfnisorientierte Konfigurationsmöglichkeiten
- Frühzeitige Erkennung von potenziellen Störungen



### Wollen agieren statt reagieren

«Die langjährige Erfahrung von terreActive im Bereich Monitoring war für uns von unschätzbarem Wert und hat einen wesentlichen Beitrag zum Erfolg dieses Projektes geleistet. tacMON sorgt dafür, dass unsere Systeme heute viel stabiler laufen und sich abzeichnende Probleme frühzeitig erkannt werden.» Rolf Stöckli, Leiter Datacenter, Ringier AG

#### Projekt:

System Monitoring

Die wichtigsten Vorteile in unserer Zusammenarbeit sieht Herr Stöckli wie folgt:

- Professionelle Monitoring-Lösung steigert Effizienz
- Verbesserte Sicherheit und Betriebsqualität
- Spürbar stabilere IT-Infrastruktur
- Transparentes und objektives Reporting
- Frühzeitige Erkennung von potenziellen Störungen
- Alarmierung per Handy in kritischen Situationen

Des Weiteren stehen Ihnen unter angegebenem Link Success Stories zu Aspectra, sourcag und Basler Kantonalbank zur Verfügung.

**Lesen Sie die kompletten Stories unter:**

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

# Produkte News

## tacMON und tacLOG weiterentwickelt

Aus unserer Entwicklungsabteilung kommen gleich zu beiden unserer Kernprodukte - tacLOG und tacMON - Neuerungen. Diese verschaffen Ihnen nicht nur auf einfache Weise den Überblick über die Konfigurationsdateien sondern ermöglichen auch ein Anpassen von mehreren Parametern «mit einem Click».

### tacLOG CCM - Central Configuration Management

Zentrale Administration: Die Konfigurationsdateien können zentral verwaltet und automatisch den gewünschten tacLOG Systemgruppen zugewiesen werden. Neue Systeme werden einfach und schnell in Betrieb genommen.

Web-Editor: Alle relevanten Konfigurationsdateien können direkt über den Web-Browser bearbeitet und Profilen zugeordnet werden.

Das Zusatzmodul wird wie folgt lizenziert:

- tacLOG CCM Central = CHF 5000.-
- tacLOG CCM Proxy = CHF 2000.-

Systems list				
[ v ]	Config. Name	Type	State	Description
<input type="checkbox"/>	ccm-prod-central	Central	Productive	Central System
<input type="checkbox"/>	ccm-prod-central-proxy1	Proxy	Productive	Proxy Zurich
<input type="checkbox"/>	ccm-prod-proxy2	Proxy	Productive	Proxy Tokio

Verwaltung von Systemgruppen und Konfigurationsverteilung

## tacMON 2.18 Erweiterungen

Power Search: Suchen von Systemen oder SNMP-Scannern aufgrund beliebiger System- oder Scanner-Suchkriterien.

Mass Edit: Anpassen von mehreren Parametern einer beliebig grossen Menge von Systemen oder SNMP-Scannern.

tacMON 2.18 ist nicht kostenpflichtig, einzig der Aufwand für den Update muss budgetiert werden. Fragen Sie uns für einen unverbindlichen Kostenvoranschlag an.

**Listing 4 Systems : Modify Search | Hide Edit Form | Delete Selected Systems**

Basic Association SNMP

	Value	Apply?
System Description	<input type="text"/>	<input type="checkbox"/>
Type	firewall TFX PAB1 (x86)	<input type="checkbox"/>
Status	activate	<input type="checkbox"/>
Room	<input type="text"/>	<input type="checkbox"/>
Rack	12.5.3	<input checked="" type="checkbox"/>
Position	<input type="text"/>	<input type="checkbox"/>
Placement	<input type="text"/>	<input type="checkbox"/>
Version	<input type="text"/>	<input type="checkbox"/>
Map	<input type="text"/>	<input type="checkbox"/>
Inventory	<input type="text"/>	<input type="checkbox"/>

Update

Select All | Select None | Columns...

Apply? ⇅	ID ⇅	System Name ⇅	System Description ⇅	Type ⇅	State ⇅	Assigned To Projects ⇅
<input checked="" type="checkbox"/>	1	taa_mon1	tacMON probe intranet	system Linux 2.4 x86	active	tA Servers
<input checked="" type="checkbox"/>	111	taa_mon2	tacMON probe jot zone	system Linux 2.4 x86	active	tA MSS Pager Alarmed Systems tA Servers
<input checked="" type="checkbox"/>	155	taa_mon3	tacMON probe internet	system Linux 2.4 x86	active	tA MSS Pager Alarmed Systems
<input checked="" type="checkbox"/>	1058	taa_vmw2-tmonol	tacMON online	system Linux 2.4 x86	active	tA Servers

Eigenschaften

Erfahren Sie mehr zu den Neuerungen in den Factsheets auf unserer Homepage und im Gespräch mit Ihrem terreActive-Ansprechpartner.

### Weitere Informationen:

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

### Factsheet:

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

# Produkte News

## tacLOG-Training nun auch für Advanced-Benutzer

**Sind Sie ein erfahrener tacLOG-Benutzer und beherrschen Sie die Konfiguration von «Simple Events»? Dann Nutzen Sie unser neues Advanced-Training.**

### Von Basic zu Advanced

Seit Herbst 2008 führen wir regelmässig tacLOG-Trainings «Basic» durch. Teilnehmer äusserten anschliessend das Bedürfnis nach einem Advanced-Training. In der Zwischenzeit hat unsere Kursleiterin Frau Diana von Bidder ein solches aufgebaut und vor wenigen Tagen das erste Training dazu durchgeführt.

### Ihr Profit: «learning by doing»

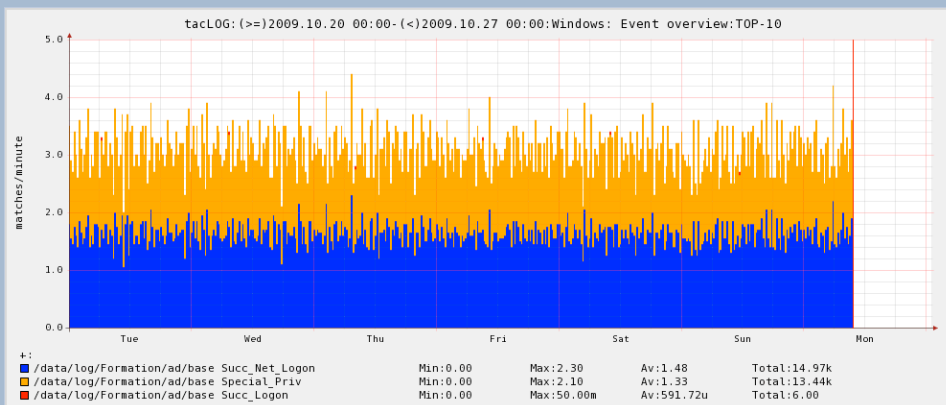
Wie immer liegt der Profit unserer Trainings im «learning by doing». Die Teilnehmer werden nicht zwei Tage mit Theorie berieselt sondern sind selbst aktiv. Während dem Grossteil der Zeit sind sie in der eigens für das Training gegründeten virtuellen Firma reale Programme am schreiben und testen sowie Unklarheiten und Probleme mit der Kursleiterin zu analysieren und lösen.

### Trainingsinhalt

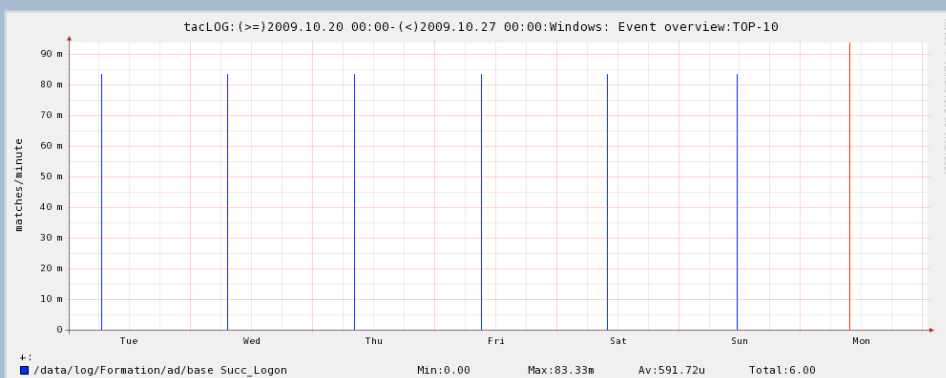
- Einführung
  - Repetition «Simple Events»
- Kontextbasierte Events
  - Theorie
  - Beispiele
  - Übungen
- Postprocessor
  - Theorie
  - Beispiele
  - Übungen
- Graphical Statistics Module (GSM)
  - Theorie
  - Beispiele
  - Übungen

**Interessiert? Erfahren Sie mehr unter:**

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



Durch die graphische Darstellung können Logs einfach virtualisiert werden. Im vorliegenden Beispiel wurden so gewisse Windows Events dargestellt.



Durch Filtering und Zooming können dann zum Beispiel selten auftretende Events hervorgehoben werden. Dies ermöglicht es auch die zu analysierenden Logdaten einzuschränken.

# Über terreActive AG

## security zone'09 – Fokus auf MSS

**Managed Security Services ist unser Fokus-Thema 2009 – auch an der diesjährigen security zone-Teilnahme. Zusammen mit dem Sourcing-Spezialisten atrete ag boten wir - in der Lounge und am Workshop - Interessierten die Möglichkeit sich Wissen aus erster Hand zu beschaffen.**

### Der Workshop

Auf Anfrage des Veranstalters führten wir den halbtägigen Workshop zum Thema Managed Security Services durch. Den besonderen Mehrwert für die Teilnehmer schafften wir mit dem Einbezug des «Make or Buy»-Aspekt. Dazu konnten wir als Referenten den Sourcing-Spezialisten atrete ag gewinnen.

### Die atrete ag

Die Spezialisten aus Zürich unterstützten nicht nur den Workshop, sondern standen den Besuchern auch in der gemeinsamen Lounge Red und Antwort.



## Security Breakfast Zürich – IT-Outsourcing der Bank von Roll AG

**IT-Outsourcing in der Finanzbranche – Aufbau und Betrieb der Bank von Roll AG. Unter diesem Titel luden wir Anfangs November ins Park Hyatt in Zürich ein. Ein Thema das interessierte.**

### IT-Outsourcing auf der grünen Wiese

terreActive baute auf der grünen Wiese eine vollständige Banken-IT-Infrastruktur – mit Ausnahme des „Core Banking“ – auf. Von der Konzeption und Umsetzung der Architektur bis hin zur Bestellung sämtlicher Hardware übernahmen wir für die Bank von Roll AG alle Tätigkeiten. Die Bank setzte uns mit 6 Monaten für die Planung und Inbetriebnahme der gesamten IT eine kurze Frist. Das Ziel, anfangs Februar 2009 den Bankbetrieb aufzunehmen, wurde erreicht.

### Kunden-Erfahrung

Wie an unseren Security Breakfasts üblich, berichten wir nicht nur über eine unserer Dienstleistungen oder Lösungen, sondern stellen den Teilnehmern – zusammen mit einem Kunden - auch gleich ein konkretes Projekt vor. Die Erfahrung des Kunden ist für die Teilnehmer jedes Mal von grossem Interesse. Und in diesem speziellen Fall sowieso.



# Über terreActive AG

## terreActive investiert in die Mitarbeiter von Morgen und unterstützt ETH-Praktika

**Seit einigen Jahren engagiert sich terreActive als Arbeitgeber von ETH-Praktika-Absolventen. In den Bereichen Development und Consulting erhalten die Studenten die Möglichkeit ihr Studiums-Know-how unter Beweis zu stellen und mit Erfahrungen aus der Praxis zu ergänzen. Seit September haben wir für 6 Monate in beiden Bereichen je einen Studenten. Wir freuen uns Andres Bühlmann und Amin Baumeler eine lehrreiche und interessante Zeit zu bieten. Lesen Sie selbst was die beiden über ihr Praktikum berichten.**

### **Andres Bühlmann, Development-Praktika**

Im September 2009, nach erfolgreichem Abschluss des Bachelor in Informatik an der ETH Zürich, habe ich mein Praktikum bei terreActive begonnen. Nach drei Jahren eher theoretischer Natur an der ETH war es für mich an der Zeit, einen tieferen Einblick in die Praxis zu gewinnen. Meine Praktikumsaufgabe besteht darin, das Open-Source Projekt Smokeping in das bestehende Produkt tacMON zu integrieren.

Im Anschluss an eine kurze Einarbeitungsphase hatte ich die Gelegenheit, mich in den Source-Code von Smokeping einzulesen und mögliche Schnittstellen für die Integration zu finden und zu bewerten. Das nächste Ziel war, das Produkt tacMON kennen zu lernen. Dies stellte aufgrund des für mich ungewohnten Umfangs und der damit verbundenen Komplexität eine gewisse Herausforderung dar, welche dank der Kompetenz und Hilfsbereitschaft des Entwicklungsteams gut gemeistert werden konnte.

Die Analyse von tacMON zeigte schnell auf, dass für die Integration von Smokeping in die bestehende Software Architektur Erweiterungen nötig sein werden. So hiess es das erste mal «Hands-on», was mir die Möglichkeit gab, das in den letzten drei Jahren an Software Architektur gelernte in der Praxis anwenden zu können. Trotz zahlreichen Projekten während des Studiums ist es eine interessante und herausfordernde Aufgabe, an einer solch komplexen Software weiterentwickeln zu dürfen.

Durch die wiederholten «Review Meetings» mit den Mitgliedern des Entwicklungsteams kristallisierte sich schliesslich eine Software Architektur heraus, welche nun in die Realität umgesetzt werden soll. So werde ich die nächsten Wochen mit der Erweiterung der Architektur von tacMON sowie dem Testen und Dokumentieren beschäftigt sein, bevor ich mich endgültig an die Integration von Smokeping machen werde. Auf jeden Fall sind noch einige lehrreiche Stunden und herausfordernde Aufgaben zu bewältigen, worauf ich mich freue.

### **Amin Baumeler, Consulting-Praktika**

Seit drei Jahren studiere ich Informatik an der ETH Zürich, wo ich nun kurz vor meinem Bachelor-Abschluss stehe. Das Masterstudium plane ich mit Fokus auf die IT-Sicherheit durchzuführen. Im Rahmen dieses Bachelor-Abschlusses wird ein dreimonatiges Praktikum verlangt. Da ich mich schon immer für die Sicherheit interessierte, fiel meine Wahl auf terreActive als Praktikumsfirma. Zugleich habe ich mich entschieden die Praktikumsdauer zu verdoppeln um einen tiefgründigeren Einblick in die Arbeitswelt zu gewinnen. Nach einem Bewerbungsgespräch und einem Schnuppertag bei terreActive erhielt ich erfreut eine Zusage um im September mit der Arbeit zu beginnen. Wie gewünscht durfte ich dem Consulting & Projects Team beitreten.

Zu Beginn erhielt ich eine Einführung und interne Schulungen zu den firmeneigenen Produkten. Anschliessend konnte ich mit meiner Aufgabe starten. Ziel meiner Arbeit ist, Angriffe durch Logkorrelation automatisiert zu erkennen um bei Bedarf Gegenmassnahmen einleiten zu können. Dazu führe ich auf einer virtuellen Umgebung Attacken durch und analysiere deren Spuren. Weiter kann ich mir Gedanken über komplexere Erkennungsmethoden und deren Realisierbarkeit machen. Ein wichtiges Beispiel ist die Erkennung von infizierten Kundensystemen. Dies soll nicht wie üblich beim Kunden selbst stattfinden, sondern beim Dienstleister. Hierbei konzentrieren wir uns primär auf das Thema E-Banking.

Nachdem ich mit dem Arbeiten begonnen habe verdeutlichten sich schnell die Unterschiede zwischen Studium und Arbeit. Während ich in den letzten drei Jahren kontinuierlich mit neuem Wissen konfrontiert wurde, zeichnet sich der Arbeitsalltag mehr durch die Anwendung aus. Weiter sind die zur Arbeit beiläufigen Teilaufgaben wie Dokumentieren auf keinen Fall zu vernachlässigen. Ein weiterer Unterschied zum Studium sind die lernfreien Wochenenden, die ich nun in vollen Zügen geniesse.

# Über terreActive AG

## Neue Telefonanlage – neue Telefonnummer

**Anfang Oktober 2009 haben wir unsere neue Telefonanlage in Betrieb genommen.**

Mit der neuen Anlage gehen wir einen Schritt weiter im CRM und nutzen die Möglichkeit der Verknüpfung zu unserer Datenbank.

Des Weiteren musste aus technischen Gründen die Telefonnummer geändert werden.

Die neue Nummer lautet: **062 834 00 55**

Die Support-Nummer (062 834 00 50) bleibt unverändert.



### Weitere Informationen:

[www.terreactive.ch/news](http://www.terreactive.ch/news)

## Neue Mitarbeiter

### Marketing, Sales & Products

**Kurt Aegerter**  
Senior Security Sales



Ausbildung: CAS Information  
Security Management CISSP, FHNW

Besonderes Know-how:  
Security Awareness

Hobbies: Sport, Motorrad, Reisen,  
Wandern, Höhle3-Club



### Consulting & Projects

**Patrick Berchtold**  
IT Security Consultant



Ausbildung: Dipl. Ingenieur HTL

Besonderes Know-how: Windows

Hobbies: Haustiere, Motorrad-Touren



### Managed Security Services

**Thomas Lohmüller**  
IT Security Engineer



Ausbildung: MSc ETH Inf.-Ing.

Besonderes Know-how: Open Source

Hobbies: Segeln, Musik, Kino



---

### **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.

terreActive AG Kasinostrasse 30 CH-5001 Aarau  
[www.terreactive.ch](http://www.terreactive.ch)

**Wir sichern Ihren Erfolg.**

**terreActive**  
**terreActive**  
**terreActive**  
**terreActive**