



Security
by Dinotronic.



Security Consulting.

Motivation. IT aus Leidenschaft bedeutet für uns auch, in einer Fülle von virtuellen Welten und Technologien den Menschen nicht zu vergessen. Darum interessieren uns nebst Normen und Regelungen auch Bedürfnisse, Bedenken und Ängste. Wir arbeiten in bewährten und motivierten Teams mit klaren Aufgaben- und Verantwortungsstrukturen und stellen fixe Ansprechpartner innerhalb eines Projekts zur Verfügung. **Kompetenz.** Durch unseren fundierten Leistungsausweis können wir als externer Partner komplementäres Know-how in eine Unternehmung einbringen. **Interesse.** Die präzise Analyse von Systemen und Prozessen ermöglicht die Entwicklung eines Lösungswegs im optimalen Kosten-/Nutzenverhältnis. **Verlässlichkeit.** Unsere Produktkompetenz verhilft durch die gezielte Auswahl und die Kombination von einzelnen Applikationen zu einer individuellen Lösung. **Herstellernähe.** Unser direkter Kontakt zu Herstellern und Kompetenzpartnern garantiert auch bei komplexen Aufgabenstellungen eine flexible und effiziente Lösungsentwicklung.

Gateway Security.

Integrated Firewall/VPN Solutions. Integrierte Unified Threat Management Lösungen decken dynamische Paketfilterung, Antivirus, Intrusion Prevention, Antispam und Contentfiltering zentralisiert ab. Virtualisierungstechnologien ermöglichen die Splitting des Netzwerks in einzelne Segmente. **Remote Access Control.** Durch browserbasierte SSL-VPN-Lösungen entfallen die Installation und die Bereitstellung eines Clients für den Zugriff auf Unternehmensanwendungen und -daten. Der integrierte Anwendungsschutz über Endpoint-Scanning sichert die Integrität der Netzwerk- und Applikationsinfrastruktur. Split-Tunneling-Kontrollen erlauben die Blockierung von Netzwerkwürmern. Spezifische Remote-Policies begünstigen die Einhaltung von Nutzungsrichtlinien. **Content Publishing.** Securitygateways mit hybrider Proxy-Firewall-Architektur ermöglichen die mehrdimensionale Überprüfung von Inhalten und garantieren deren flexible Bereitstellungsoptionen bei höchster Verwaltbarkeit, Verfügbarkeit und Skalierbarkeit.

Endpoint Security.

Endpoint Protection. State-of-the-Art Applikationen für Client Firewall, Antivirus und Proactive Threat Protection schützen auch vor komplexen Angriffen wie Rootkits, Zero-Day Angriffen und Spionageprogrammen. **Encryption.** Verschlüsselungskonzepte erlauben sektor- und dateibasierte Verschlüsselung ganzer Datenträger über eine zentrale Managementkonsole. **Port Protection.** Integrierte Lösungen kontrollieren physikalische und drahtlose Schnittstellen genauso wie externe Speicher und ermöglichen eine individualisierte Rechtevergabe. **Data Loss Prevention.** Leistungsfähige Systeme überprüfen alle Datenoperationen nach Aussen in Echtzeit und verhindern unerlaubte Übertragung von Unternehmensdaten. **Network Access Control.** Überwachungsprogramme blockieren nichtkonforme Geräte und verhindern Zugriff auf Netzwerkressourcen.

Mail Security.

Mail Appliances. Ausfallsichere Hard- und Softwaresysteme für Antispam, Virenschutz und fortschrittliches Content Filtering erlauben den Schutz vor bössartigen Bedrohungen durch ein- oder ausgehende E-Mail- und Instant Messaging-Korrespondenz. Durch den strukturierten Ansatz lassen sich vertrauliche Daten besser kontrollieren, die mit Datenlecks verbundenen Risiken effektiver bewältigen und gesetzliche sowie unternehmensinterne Richtlinien besser einhalten. **Mail Encryption.** S/MIME, OpenPGP und TLS gewährleisten die Verschlüsselung und Signatur von E-Mail an zentraler Stelle im Unternehmensnetzwerk. PDF-Technologien stellen die Anbindung externer Kommunikationspartner ohne Sicherheitsinfrastruktur sicher. **Mail Storage Management.** Weitreichende Archivierungslösungen erlauben die Speicherung und Verwaltung von Daten aus E-Mail-Systemen, Datei-Server-Umgebungen und Instant Messaging-Plattformen. Klassifizierungsmethoden ermöglichen die Kategorisierung und Indexierung der Zieldaten.

Infrastructure by Dinotronic.

Die Zukunft liegt im Netzwerk. Aufgrund detaillierter Bedarfsanalysen entwickeln wir aus hochqualitativen Komponenten massgeschneiderte Individuallösungen. Dabei legen wir grossen Wert darauf, traditionell gewachsene Strukturen möglichst sanft – aber wirkungsvoll – an neueste Technologien anzupassen. Als Spezialist für die Integration komplexer Client-/Server-Systeme decken wir das gesamte Leistungsspektrum ab: Von der Projektierung über das Beschaffen von Hard- und Software bis zur Implementation und Dokumentation.

Hosting by Dinotronic.

Der Arbeitsplatz ist überall. Unsere Hosting-Lösungen für Exchange, Mail Security, Office und Individualapplikationen werden dem modernen Arbeitsverhalten gerecht, erhöhen die Datensicherheit und senken gleichzeitig die Kosten für Anschaffung, Aktualisierungen und Support. Eine Hosting-Plattform der neuesten Generation in einem externen Rechenzentrum und unsere Flexibilität bei der Erarbeitung von individuellen Lösungen werden auch höchsten Komfort- und Sicherheitsansprüchen gerecht.

Security by Dinotronic.

Fortschritt hat seine Schattenseiten. Kaum ein Tag vergeht, bis neu entwickelte Technologien nicht nur genutzt, sondern auch missbraucht werden. Wir arbeiten darum täglich an innovativen Lösungen, um sensible Daten optimal zu schützen – ohne Funktionalitäten zu beeinträchtigen – und so dem Unerwünschten die Türen weit vor der Nase zuzuschlagen. Dabei bauen wir auf unseren Sachverstand, unsere Beratungskompetenz, eine ausgewogene Palette von hervorragenden Produkten und unseren Weitblick für neue Wege.

Software Development by Dinotronic.

Individualität kennt keine Grenzen. Bei der Entwicklung von branchenspezifischer Software, der Anpassung und Weiterentwicklung bestehender Applikationen, der Neuentwicklung von Software und der spezifischen Erweiterung von Sharepoint- und Security-Lösungen gibt es nur einen einzigen Massstab: Die Individualität unserer Kunden. Unsere interne Entwicklungskompetenz und der direkte Kontakt zu Herstellern und Partnern garantieren dabei eine effiziente und zukunftssichere Umsetzung.

Mit Sicherheit praxistauglich.

Security Consulting.

Mit Sicherheit gut beraten.

Die Herausforderung.

Durch immer heterogener werdende Infrastrukturen, den erhöhten Anspruch an Mobilität und verschärften gesetzlichen Bestimmungen steigt der Bedarf nach integrierter IT-Sicherheit fast täglich. Trotzdem soll die Benutzerfreundlichkeit nicht beeinträchtigt werden und eine zentrale und einfache Administration möglich sein. Dabei sind die Bedürfnisse so individuell wie die Kunden und Geschäftsprozesse selbst.

Die Kundenlösung.

Aufgrund einer detaillierten Bedarfsanalyse wird unter Berücksichtigung des optimalen Kosten-/Nutzenverhältnisses eine zukunftssichere und möglichst zentral administrierbare Lösung ausgearbeitet. Dabei wählt Dinotronic herstellerunabhängig die jeweils optimal passenden Applikationen aus und vereint diese – bei Bedarf durch individuelle Anpassungen – zu einer integrierten Lösung. Durch Service- und Wartungsverträge wird die effiziente Betreuung im Supportfall gewährleistet.

Der Kundennutzen.

Dinotronic verfügt über langjährige Erfahrung bei der Analyse von komplexen Fragestellungen, der Projektierung von individuellen Lösungen und der effizienten Umsetzung. Die zum Einsatz kommenden Produkte stammen von etablierten Herstellern, welche eine führende Rolle bei der Entwicklung von Sicherheitslösungen einnehmen. Durch unsere Herstellernähe profitiert der Kunde nicht nur von einer aussergewöhnlichen Produktkompetenz, sondern auch von Flexibilität und Effizienz bei der Lösung von komplexen Problemstellungen und Supportfällen.

Gateway Security.

Mattig-Suter & Partner, Schwyz.

Die Herausforderung.

Für die Automatisierung der Datenerfassung im Risk-Management soll eine einfach zu handhabende Lösung gefunden werden, die den hohen Sicherheitsanforderungen und gesetzlichen Richtlinien im Treuhandwesen gerecht wird und gleichzeitig den Know-how Transfer vom Unternehmen zu Partnern und Kunden reguliert. Die Automatisierung soll sich durch hohe Benutzerfreundlichkeit und geringe clientseitige Anforderungen auszeichnen.

Die Kundenlösung.

Basis der Lösung bildet der Citrix Access Gateway. Im Zusammenspiel von Endpoint-Scanning und Smart-Access werden nicht nur die allgemeinen Zugriffsrechte für das Firmennetz geregelt, sondern auch die Bearbeitungsmöglichkeiten der zur Datenerfassung bereitgestellten Excel-Datei festgelegt. Dabei berücksichtigt die Lösung unterschiedlichste Zugriffsszenarien durch fein differenzierte Bearbeitungsprofile.

Der Kundennutzen.

Trotz erhöhter Automatisierung ist für den Kunden der Schutz des eigenen Know-hows gewährleistet. Durch die innovative SSL-VPN Verbindung sind auf Clientseite keinerlei Softwareinstallationen oder spezifische Konfigurationen nötig. Die Datenerfassung und -übermittlung erfolgt browserbasiert und zeichnet sich durch eine hohe Benutzerfreundlichkeit aus. Clientseitig werden keine lokalen Daten produziert und gespeichert.

Die Technik im Überblick

- Citrix Access Gateway Model 2010 Appliance
- Citrix Access Gateway Standard Edition
- Citrix Presentation Server Advanced

Endpoint Security.

Schroders, Zürich.

Die Herausforderung.

Für die Absicherung und Verschlüsselung von mobilen Endgeräten soll eine Lösung gefunden werden, die sich durch überdurchschnittliche Usability, ein optimales Preis-/Leistungsverhältnis und eine zentrale Managementkonsole auszeichnet. Die Installation der Lösung soll innerhalb eines Arbeitstages möglich sein. Nebst der effizienten Projektumsetzung ist dem Kunden eine einfache Supportlösung ein zentrales Anliegen.

Die Kundenlösung.

Der Kunde entscheidet sich aufgrund der hohen Skalierbarkeit, der Benutzerfreundlichkeit und des Preis-/Leistungsverhältnisses für Utimaco SafeGuard Enterprise 5.2. Dinotronic zeichnet verantwortlich für die Planung, die Budgetierung, die Umsetzung des Projekts und den Produktesupport. Nach einer Testinstallation werden innerhalb eines Arbeitstages rund 20 Clients konfiguriert und die Mitarbeitenden geschult.

Der Kundennutzen.

Der Kunde profitiert durch die neue Lösung von erhöhter Endpoint-Sicherheit. Das Management der einzelnen Clients wird durch eine benutzerfreundliche zentrale Konsole stark vereinfacht. Die modulare Systemarchitektur und die offenen Schnittstellen zur IT-Infrastruktur gewährleisten die Skalierbarkeit. Der hohe Automatisierungsgrad garantiert tiefere Kosten gegenüber herkömmlichen Lösungen für Rollout und Unterhalt.

Die Technik im Überblick

- Utimaco SafeGuard Enterprise 5.2
- Windows 2003 Server
- SQL 2005 Server

Mail Security.

mammut soft computing ag, Oberentfelden.

Die Herausforderung.

Für die elektronische Korrespondenz im banknahen Umfeld gelten dieselben Sicherheitsbestimmungen wie für Banken selbst. Die einzelnen Benutzer sollen – trotz unterschiedlichster Kommunikationspartner – keine Entscheidungsbefugnis über das Regelwerk für die Verschlüsselung und die digitale Signatur der E-Mail haben. Die Steuerung sämtlicher Sicherheitsmassnahmen soll zentral am Gateway erfolgen.

Die Kundenlösung.

SafeGuard MailGateway integriert die Prozesse der Ver- und Entschlüsselung sowie der elektronischen Signatur an zentraler Stelle im Unternehmensnetzwerk. Bestehende E-Mail basierte Workflow-Prozesse bleiben dadurch erhalten. Empfängerabhängig verwendet die Applikation die etablierten Standards S/MIME und OpenPGP. Für die Kommunikation mit Partnern ohne Sicherheitsinfrastruktur wird eine passwortbasierte PDF-Verschlüsselung eingesetzt.

Der Kundennutzen.

Durch die zentrale Steuerung aller Prozesse haben die einzelnen Clients wahlweise nur noch beschränkter Einfluss auf den Verschlüsselungs- und Signaturvorgang. Sicherheitsrichtlinien werden dadurch automatisch korrekt umgesetzt. Die Wahl des adäquaten Verschlüsselungsstandards erfolgt zentralisiert am Gateway – abhängig vom empfangenseitigen Standard. Eine Schulung der Mitarbeitenden zur Handhabung von Verschlüsselung und Signatur entfällt.

Die Technik im Überblick

- Utimaco SafeGuard MailGateway

Alexander Villiger, Sales



villiger@dinotronic.ch
Symantec Sales Professional (SSP), 20 Jahre Verkaufserfahrung mit Spezialgebiet Endpoint Security/DLP.

Andreas Höfler, Senior Consultant



hoefler@dinotronic.ch
Informatikerlehre bei Deutsche Telekom. Tätigkeit im Security-Bereich. Schwerpunkte: Symantec Endpoint Protection und SafeGuard Enterprise.

Daniel Senn, Senior Consultant



senn@dinotronic.ch
Über 18 Jahren Erfahrung in allen Bereichen der IT – von Endpoint Security bis zu anspruchsvollen Gateway- und DLP-Lösungen.

Detlev Pacholke, Presales Consultant



pacholke@dinotronic.ch
Seit 15 Jahren als IT Presales Consultant und Trainer. MCSE Security, Schwerpunkt Datenverschlüsselung und Mobile Access.

Dino Fiori, Senior Consultant



fiori@dinotronic.ch
Geschäftsführer, Studium der Wirtschaftsinformatik, Uni Zürich. CISSP. 16 Jahre IT-Erfahrung.

Michael Hausmann, Sen. Account Manager



hausmann@dinotronic.ch
Partner der Geschäftsleitung, Ausbildung als Elektromonteur bei Elektro Kisseleff AG. Weiterbildungen in Support und IT-Beraterung. 15 Jahre IT-Erfahrung.

Michael Schweizer, Senior Consultant



schweizer@dinotronic.ch
Studium der Wirtschaftsinformatik an der Universität Zürich. MCSE Security.

Nicole Wieland, Project Manager



wieland@dinotronic.ch
Ausbildung als Informatikerin mit eidg. Fachausweis. Weiterbildungen in den Bereichen Microsoft (MCSE) und Citrix. 8 Jahre IT-Erfahrung.