

# VSE NET

Telsis Customer Experience



Telsis

Wie VSE NET auf der Startseite seiner eigenen Website klar angibt, ist der Telekommunikationsmarkt ‚im Wandel‘. Neue Technologien verändern die Art und Weise, wie Netzbetreiber, wie VSE NET, ihre Dienstleistungen für ihre Kunden erbringen. Der Wechsel zu softwarebasierten IP-Netzen reduziert die Kosten und ermöglicht es den Netzbetreibern, ihr Angebot an Telekommunikationsdienstleistungen zu erweitern. Dies bietet allerdings auch neue Möglichkeiten für Betrüger und Hacker. Dieser Anwenderbericht beleuchtet, wie VSE NET in Zusammenarbeit mit Telsis das Problem des Telefonbetrugs in seinem Netz festgestellt und gelöst hat.

VSE NET GmbH ist ein regionaler Telekommunikationsanbieter mit Sitz im Saarland und Teil des deutsch-luxemburgischen artelis-Konzerns, der im Besitz der Energieanbieter VSE AG und Enovos International S.A. ist. Das Leistungsspektrum der VSE NET reicht von der Bereitstellung von Daten-, Internet- und Sprachdiensten über die Vermietung hochsicherer Rechenzentrumsflächen bis hin zur Planung, Bau und Betrieb eines gesamten Telekommunikationsnetzes. VSE NET bietet seine Leistungen vorwiegend Geschäftskunden wie Krankenhäusern, Verwaltungen, Universitäten, Callcenter, Banken und Versicherungen an. Darüber hinaus werden auch von anderen Festnetz- und Mobilfunknetzbetreibern die Dienstleistungen der VSE NET angeboten.

Der Geschäftsführer von VSE NET, Michael Leidinger, leitet das Unternehmen seit seiner Gründung im Jahr 1998. Er hat das Wachstum des Unternehmens begleitet und das Netz so weit ausgebaut, dass mittlerweile mehr als eine Milliarde Sprachminuten pro Jahr gezählt werden. Für Michael Leidinger sind Innovationen eine wesentliche Voraussetzung, damit VSE NET seine Position auf dem deutschen Telekommunikationsmarkt beibehalten und weiter ausbauen kann. Wie er sagt:

*„Traditionelle Telekom-Dienste werden immer günstiger und damit die Gewinnspannen immer geringer. Innovationen sind äußerst wichtig, damit unser Geschäft auch in Zukunft wächst. Wir wollen, dass unsere Kunden VSE NET als innovatives Unternehmen erleben, das kontinuierlich neue Produkte bereitstellt, die vom sich wandelnden Markt nachgefragt werden. In den letzten Jahren haben wir massiv in Cloud-Dienste in Virtualisierung, Sicherheit und Machine-to-Machine-Dienste (M2M) (automatisierter Informationsaustausch zwischen Endgeräten) investiert. Dies hilft uns, unsere Spitzenposition am Markt zu behaupten.“*

Die Zusammenarbeit mit Technologiepartnern ist für VSE NET äußerst wichtig, um das Innovationsversprechen zu erfüllen. Seit mehr als sechs Jahren arbeiten VSE NET und Telsis zusammen, um den Kunden innovative und hochwertige Dienste anzubieten. Zu Beginn half Telsis mit Local Number Portability und Least-Cost-Routing-Diensten (automatische Auswahl des preiswertesten Telefonanbieters), um die operativen Kosten zu optimieren. Mittlerweile verwendet VSE NET die Telsis Ocean Services Plattform (OSP), um hochentwickelte, intelligente Dienste zu erbringen. Michael Leidinger beschreibt OSP folgendermaßen:

*„Telsis ist das Gehirn in unserem Netzwerk. Es bietet die Intelligenz, die es uns ermöglicht, unseren Kunden innovative Dienste bereitzustellen.“*

Das Telsis-‚Gehirn‘ wird mittlerweile auch verwendet, um das Problem des Telefonbetrugs innerhalb des Netzes der VSE NET zu adressieren.

## Betrugsschutz

Die Muttergesellschaft von VSE NET hat seit Langem interne Regeln für Daten- und Betrugsschutz etabliert und VSE NET war immer ein Vorreiter, diese Probleme zu identifizieren und zu lösen.

Vor zwei Jahren erkannte VSE NET, dass die PBX (Private Branch Exchange oder Nebenstellenanlage) eines seiner Geschäftskunden manipuliert wurde. Zur etwa gleichen Zeit gab es auch einen umfangreichen Hack von mehr als einer Million CPE-Geräten (Customer Premises Equipment, Teilnehmer-Endgeräte) in Deutschland. Hacker fanden heraus, dass ein Standardpasswort verwendet wurde, welches Zugriff auf diese Geräte ermöglichte, da die Kunden selten das Standardpasswort des Gerätes veränderten. Diese Ereignisse führten zu einem starken Anstieg von Betrugsangriffen im Netz und Hacker manipulierten diese Geräte, um betrügerische Anrufe zu tätigen.

VSE NET stellte fest, dass das Problem erheblich war und dass es unbedingt gelöst werden musste. Wie Michael Leidinger sagte:

*„Wir schätzen, dass die Auswirkungen des Angriffs direkte Kosten in der Höhe von 100 000 € – 200 000 € verursachten.“*

Zunächst analysierte VSE NET sein Abrechnungssystem, um Betrugsmuster festzustellen. Das System stellte allerdings erst eine Stunde nach Abschluss der Anrufe relevante Informationen zur Verfügung. Die Call Data Records (CDRs, Kommunikations-

---

*“Telsis ist das Gehirn in unserem Netzwerk. Es bietet die Intelligenz, die es uns ermöglicht, unseren Kunden innovative Dienste bereitzustellen.“*

Michael Leidinger, Managing Director, VSE NET

---

datensätze) wurden analysiert, um betrügerische Muster wie beispielsweise ungewöhnlich viele Anrufe pro Zeiteinheit außerhalb der Geschäftszeiten zu einer internationalen Mehrwertrufnummer festzustellen. (Dies weist auf einen wahrscheinlichen PBX-Hack hin). Bei der Analyse der CDRs wurden zwar betrügerische Muster festgestellt, aber der Betrug konnte erst bestimmt werden, nachdem er stattgefunden hatte. Wie Michael Leidinger sagt:

*„Die Verwendung der CDR Analyse war hilfreich, um Betrugsmuster festzustellen. Wir benötigten allerdings eine Lösung, die proaktiv und nicht nur reaktiv arbeitet.“*

VSE NET entwickelte anfänglich das Konzept und beauftragte Telsis mit der Umsetzung, da die Ocean Services Platform das Routing sowohl im älteren TDM- (Time Division Multiplexing) als auch im modernen IP-Telefonnetz (Internet Protocol) direkt durchführte. Das Ziel war, einen Algorithmus zu entwickeln, der diese betrügerischen Muster in Echtzeit feststellen würde, um die betrügerischen Anrufe sofort zu beenden. Damit würde es möglich sein, einen proaktiven Schutz anzubieten, statt nur im Nachhinein darauf zu reagieren. Telsis Voice SafeGuard wurde für VSE NET die Lösung für Betrugsschutz.

Bei der Implementierung von Voice SafeGuard konnte VSE NET die Wirksamkeit beider Methoden für einen Zeitraum von zwei Monaten vergleichen. VSE NET stellte durchschnittlich drei bis vier Angriffe pro Monat fest. Michael Leidinger erklärte die Auswirkungen von Voice SafeGuard:

---

*„Als wir die Daten beider Methoden analysierten, stellten wir fest, dass sich nach Einführung von Voice SafeGuard die Betrugsfälle um den Faktor 100:1 reduzierten. Ein typischer Betrugsangriff kostete uns früher im Durchschnitt 1 000 € und wir konnten die Kosten auf nur 13 € reduzieren.“*

Michael Leidinger, Managing Director, VSE NET

---

*„Als wir die Daten beider Methoden analysierten, stellten wir fest, dass sich nach Einführung von Voice SafeGuard die Betrugsfälle um den Faktor 100:1 reduzierten. Ein typischer Betrugsangriff kostete uns früher im Durchschnitt 1 000 € und wir konnten die Kosten auf nur 13 € reduzieren.“*

VSE NET sieht die zentrale Routing-Komponente des Netzes als den idealen Ort, um Betrug zu unterbinden. Die Telsis-OSP mit Voice SafeGuard wird seit Oktober 2015 im Netz der VSE NET eingesetzt.



Michael Leidinger, Managing Director, VSE NET

---

„Voice SafeGuard hat uns geholfen, unsere Position als das sicherste und verlässlichste Netz zu stärken. In Zukunft wird Sicherheit zu einem noch wichtigeren Geschäftsfeld werden und dann sind wir in einer guten Position, um neue auf Sicherheit bedachte Kunden in Deutschland und Luxemburg zu gewinnen.“

---

Michael Leidinger, Managing Director, VSE NET

Wie Michael Leidinger sagt:

*„Voice SafeGuard funktioniert in unserem Netz stabil und verlässlich. Es reduziert die Verluste sowohl für uns als auch für unsere Kunden.“*

Mit der Lösung Voice SafeGuard konnte VSE NET auch seine Innovationsfähigkeit auf dem Markt beweisen und seinen Ruf als Netzbetreiber von sicheren Telefondienstleistungen für Geschäftskunden erheblich verbessern. Voice SafeGuard ist ebenfalls integrierbar in Cloudlösungen und virtualisierte Strukturen. Wie Michael Leidinger erklärt:

*„Wir sehen Voice SafeGuard als ein perfektes Werkzeug, um unseren Ruf als sicherer Anbieter für Geschäftskunden zu wahren.“*

## Wie sieht die Zukunft aus?

Innerhalb der nächsten fünf Jahre erwartet VSE NET, dass das ältere TDM-Telefonnetz abgebaut und vollständig mit einem modernen IP-basierten Netz ersetzt wird. VSE NET beabsichtigt den Vorteil als Innovationsführer zu nutzen und sich bei Marketingmaßnahmen als der sicherste Anbieter von Telefon- und Datendienstleistungen zu positionieren. Michael Leidinger blickt optimistisch in die Zukunft:

*„Voice SafeGuard hat uns geholfen, unsere Position als das sicherste und verlässlichste Netz zu stärken. In Zukunft wird Sicherheit zu einem noch wichtigeren Geschäftsfeld werden und dann sind wir in einer guten Position, um neue auf Sicherheit bedachte Kunden in Deutschland und Luxemburg zu gewinnen.“*

VSE NET ist bereit auch in Zukunft die Weiterentwicklung von Voice SafeGuard zu unterstützen und die Lösung in anderen Bereichen anzuwenden, um neue Betrugsformen zu erkennen und zu bekämpfen.

Bei der kontinuierlichen Erweiterung des Dienste- und Lösungsportfolio, um die Innovationskraft für ein zukunftsfähiges Netz weiter zu stärken, ist Telsis für die VSE NET ein verlässlicher Partner mit neuen Ideen für intelligente Netze der Zukunft.

---

Contact: [contactus@telsis.de](mailto:contactus@telsis.de)

UK  
T: +44 (0) 1489 76 00 00

Germany  
T: +49 (0) 6151 827 850

Copyright © 2016. Telsis Communication Services Limited. 1593-1044-01 DE  
Telsis products are subject to continual development and specifications may change. Prospective buyers should exercise their own independent judgement to confirm the suitability of our products for their particular application. Telsis, Ocean and NODAL are registered trademarks of Telsis Communication Services Ltd. All other trademarks and registered trademarks are the property of their respective holders

**Telsis**

[www.telsis.com](http://www.telsis.com)