

# Berner GmbH *Dezentrales Berechtigungsmanagement durch Squid Software Appliance*

Am 1. April 1957 eröffnet Albert Berner - im Alter von 21 Jahren - eine Schraubenhandlung im Baden-Württembergischen Städtchen Künzelsau.

Schon 1969 nimmt Albert Berners Vision einer europäischen Firmengruppe konkrete Formen an. Die ersten Tochterunternehmen in Belgien, Österreich, Frankreich und der Schweiz werden gegründet.

Auch in den Nachfolgejahren wird die Expansion in Europa weiter fortgesetzt. Es folgen 1970 Dänemark, 1971 Niederlande, 1974 Italien. 1972 gründet Albert Berner die BTI Befestigungstechnik in Ingelfingen (D).

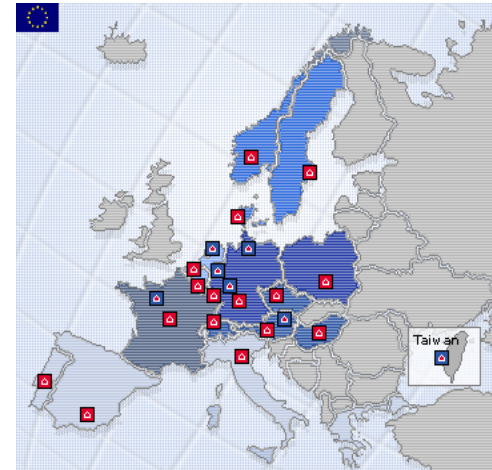
1976 übernimmt Berner eine Fabrik für Schrauben und Befestigungsteile in Taiwan. Die BernerGruppe beschäftigt derzeit mehr als 6500 Mitarbeiter.

## Anforderungen

Im Sinne einer strikten Kundenausrichtung, die eine schnelle Reaktion durch informierte Mitarbeiter erwartet, wurde eine zentrale Sicherheitsinfrastruktur für den Zugang berechtigter Mitarbeiter in das Internet bereitgestellt.

Diese Lösung erwies sich bei der Benutzerverwaltung als zu wenig agil für einen dynamischen Mittelständler. Im Rahmen der internationalen Ausrichtung war es daher notwendig, die Balance zwischen zentral bereitgestellten IT-Services und dezentralen Services neu zu bewerten und Teile der zentral bereitgestellten Services an die verbundenen Unternehmen (VBUs) zu delegieren.

Um die ca. 1.500 IT-Nutzer an den 17 europäischen Standorten dezentral zu verwalten und gleichzeitig den Netzwerkverkehr im Weitverkehrsnetz zu reduzieren, boten sich verschiedene Alternativen auf Proxy-Basis an. Um eine kostengünstige Skalierung der Proxy-Lösung zu erhalten, kamen zu kommerziellen Lösungen sehr schnell Alternativen aus dem Open-Source-Bereich ins Gespräch, da andere Lösungen weder bei den Anforderungen an die Hardware noch beim Lizenzmodell an die lokalen Anforderungen angepaßt werden können. Auf der anderen Seite wollte man keine Infrastruktur aufbauen, deren Installation und Wartung Spezialisten für Linux in den einzelnen VBUs erfordert hätte. Eine Anbindung der Authorisierung an das Active Directory von Windows erschien als eine interessante Lösung.

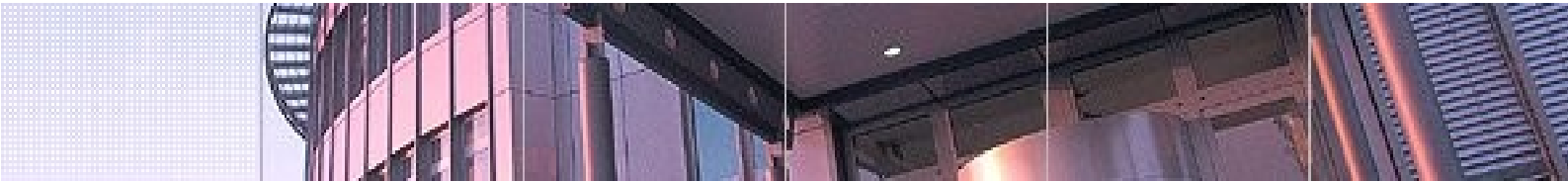


*„Die Dezentralisierung der HTTP-  
Proxies spart den VBUs Band-  
breite im „Berner European  
Network“ und gibt ihnen vor  
allem die Flexibilität bei der  
Rechteverwaltung über Windows  
zurück.“*

Peter Knoblach  
International IT  
Berner Holding

Powered by





secXtreme wurde beauftragt, ein Konzept zum Einsatz von verteilten Proxy-Systemen im Netz der Berner GmbH auf der Basis von Squid zu erstellen und umzusetzen. Im Rahmen des Konzepts wurden die besonderen Anforderungen an eine Lösung klar:

- ✓ Betrieb und Installation der Proxies auf älterer aber auch neuester Hardware
- ✓ Installation und Betrieb durch Personal ohne Linux Erfahrung
- ✓ Disaster-Recovery-fähig, Neuinstallation und Konfiguration innerhalb von 20 Minuten
- ✓ Software-Wartung als Investitionsschutz
- ✓ Unterstützung des europaweit aufgebauten Active Directory Forrests
- ✓ Transparenz für den Benutzer, gleich an welchem Standort er sich anmeldet

## Lösung

Um diese Anforderungen zu erfüllen, hat secXtreme eine Software-Appliance basierend auf der Debian-Linux Distribution entwickelt. Auf der erstellten Installations-CD wurde der gesamte Installationsprozess derart an den Verwendungszweck angepasst und durch eigene Erweiterungen ergänzt, dass bei der Installation nur noch die kundenspezifischen Einstellungen durchgeführt werden müssen. Am Ende der Installation ist das System nach einem Reboot sofort einsatzfähig.

Durch ein spezielles LDAP-Authentifizierungsmodul ist es möglich, eine Authentifizierung auch im Active Directory Forrest europaweit sehr flexibel und performant durchzuführen. Ein Merkmal, welches nicht durch vorhandene Open-Source abgedeckt werden konnte.

Um die Benutzerverwaltung im Active Directory durchführen zu können, wird ein vorhandenes LDAP-Attribut der Benutzerobjekte verwendet. Damit sind keine Erweiterungen des LDAP-Schemas notwendig. Es werden nur die Rechte des Attributs unternehmensweit restriktiv eingestellt und mit Werten belegt, welche dann die Internetberechtigung steuern. Aufgrund der Anzahl von Benutzern konnte auch diese Anpassung nur durch entsprechende Hilfsmittel geschehen, die durch secXtreme entwickelt und der Administration auf der Installations-CD bereitgestellt wurden.

Um das System selbst abzusichern, wurden Maßnahmen umgesetzt, wie sie secXtreme bei der Härtung sicherheitsrelevanter Systeme durchführt. Die Aktualisierung der Software erfolgt automatisch über das Internet. Von secXtreme entwickelte Pakete können dabei im Rahmen der Software-Pflege digital signiert auf dem Server von secXtreme zum Download bereitgestellt werden.

## Fazit

Durch eine schlüsselfertige Lösung auf Basis von Open-Source Software konnte Berner GmbH eine typische Aufgabenstellung kostengünstig und zukunftssicher realisieren.

### Über secXtreme GmbH

secXtreme GmbH ist ein Unternehmen, das sich auf die Sicherheit Ihrer Informationen spezialisiert hat. Dazu gehören die Bereiche Audit, Penetration Testing, Sicherheitsanalysen und Trainings. Neben diesen Bereichen entwickelt secXtreme wie hier für die Berner GmbH Sonderlösungen im Sicherheitsumfeld. secXtreme ist Mitglied im Deutschen CERT-Verbund und unterstützt seine Kunden bei Incident Management- und Forensik-Aufgaben.

Weitere Informationen erhalten Sie unter <http://www.sec-xtreme.com>, per E-Mail an [info@sec-xtreme.com](mailto:info@sec-xtreme.com) und per Telefon.



secXtreme GmbH  
Münchener Str. 1a  
D-82024 Taufkirchen  
Tel. +49(0)89-18 90 80 68-0  
Fax. +49(0)89-18 90 80 68-77  
E-Mail: [info@sec-xtreme.com](mailto:info@sec-xtreme.com)  
WWW: [www.sec-xtreme.com](http://www.sec-xtreme.com)