Özgür Yazılım ve Linux Günleri 2011
Bilgi Üniversitesi / İstanbul
01.04.2011

İçerik

- Bilgi Sızıntısı Nedir?
- Bilgi Sızıntısı İstatistikleri
- Türkiye ve Kişisel Veriler
- MyDLP Nedir?
- MyDLP Bileşenleri ve Yapısı
- Demo
- Sorular ve Yorumlar

Bilgi Sızıntısı Nedir?

Kurumun bilişim teknolojileri ile kullandığı, şlediği ya da ürettiği verilerin bilinçli ya da bilinçsiz bir şekilde kurum dışına taşınarak, belirlenmiş "bilgi güvenliği" politikalarının hlalidir.

Bilgi Sızıntısını Neden Engellemek Gerekir?

- Kişisel verilerin gizliliği
- Stratejik gereksinimler
  - İş gizliliği
  - Veri gizliliği
- Hukuki yükümlülükler
- Uluslararası bilgi güvenliği standart ve akreditasyonlarına uyum
  - HIPAA, GLBA, BASEL II, Sarbanes-Oxley, DSS

Problem

“Elektronik ortamlarda bilgiyi korumak zordur.”

Her türlü veri birçok yol ile dışarı çıkabilir.

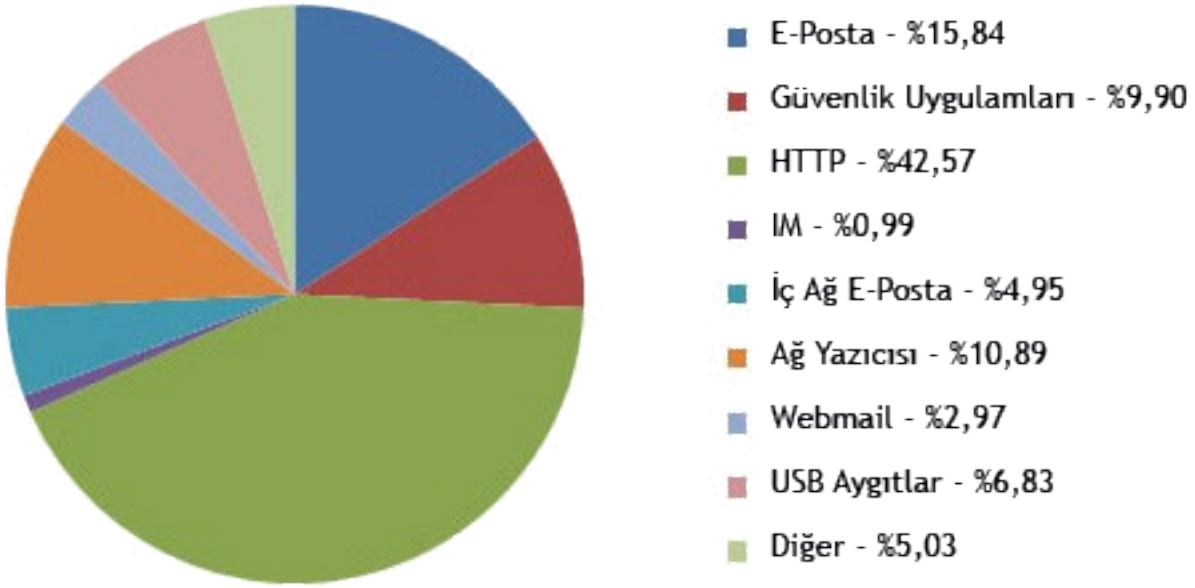
Bilgi Sızıntısı Olayları

- Bilgi sızıntısı olayları aslında her yerde.
  - KPSS sorularının çalınması
  - KEY ödemeleri sırasında kişisel verilerin umarsızca yayınlanması
  - Kişisel sağlık bilgilerinin elden ele gezmesi
  - Wikileaks

ve daha birçok örnek..

Bilgi Sızıntısı Kaynakları

- Bilgi sızıntısının %77,25'i ağ uygulamaları üzerinden gerçekleşmektedir.



Referans: http://www.surveilstar.com/prevent-data-leakage.html

Bilgi Sızıntısının Sonuçları

- Datagate: Bir bilgi sızıntısı olayının ortalama maliyeti 1,82 milyon dolar olarak hesaplandı.
  - Sayısal veriler hazırlanırken yapılan çalışmada sadece %23'lük katılım üzerinden hesaplamalar yapılırken, diğer katılımcılar bu tarz olayları takip edebilecek yada kayıpları tespit edebilecek durumda olmadıkları anlaşıldı.

Referans:
http://www.eweek.com/c/a/Security/New-Report-Chronicles-the-Cost-of-Data-Leaks/

Türkiye'de Kişisel Verilerin Gizliliği

- Mevcut herhangibir ceza yaptırımı bulunmamaktadır.
- Anayasa'nın yeni değişen 20. Maddesi diyor ki;
  - "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla islenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Türkiye'de Kişisel Verilerin Gizliliği

- 2008 Ekim ayından itibaren TBMM Adalet Alt Komisyonunda görüşülen "Kişisel Verilerin Korunması Kanun Tasarısı"nda ise başta sağlık kurumları olmak üzere kişisel veri işleyen tüm kamu ve özel kurumlara bu verileri koruma görevi verilmiştir.
- Tasarının yasalaşması ile cezai müeyyideler devreye girecek.

MyDLP Nedir?

- MyDLP bir DLP çözümüdür.
- DLP : Data Loss / Leak Prevention
- Kabaca;
  - Kurum bir bilgiyi / veri türünü gizli olarak tanımlar.
  - O bilgi / veri türü kurum dışına çık(a)maz.

- MyDLP özgür yazılımdır. GPLv3 lisansı ile dağıtılmaktadır.

- MyDLP yurtdışından oldukça büyük bir ilgi görüyor. MyDLP, Amerika'dan Yeni Zellanda'ya 80 ülkeden binlerce kişi tarafından takip ediliyor, kuruluyor, kullanıyor.

MyDLP Nedir?

- MyDLP ağ (network) üzerinden ve uçbirim üzerinden her an denetleme yapar.
- Her türlü veri akışı denetler.
- Gizli / hassas bir verinin varlığı tespit ederse, **veri akışı engeller**.

Neden MyDLP?

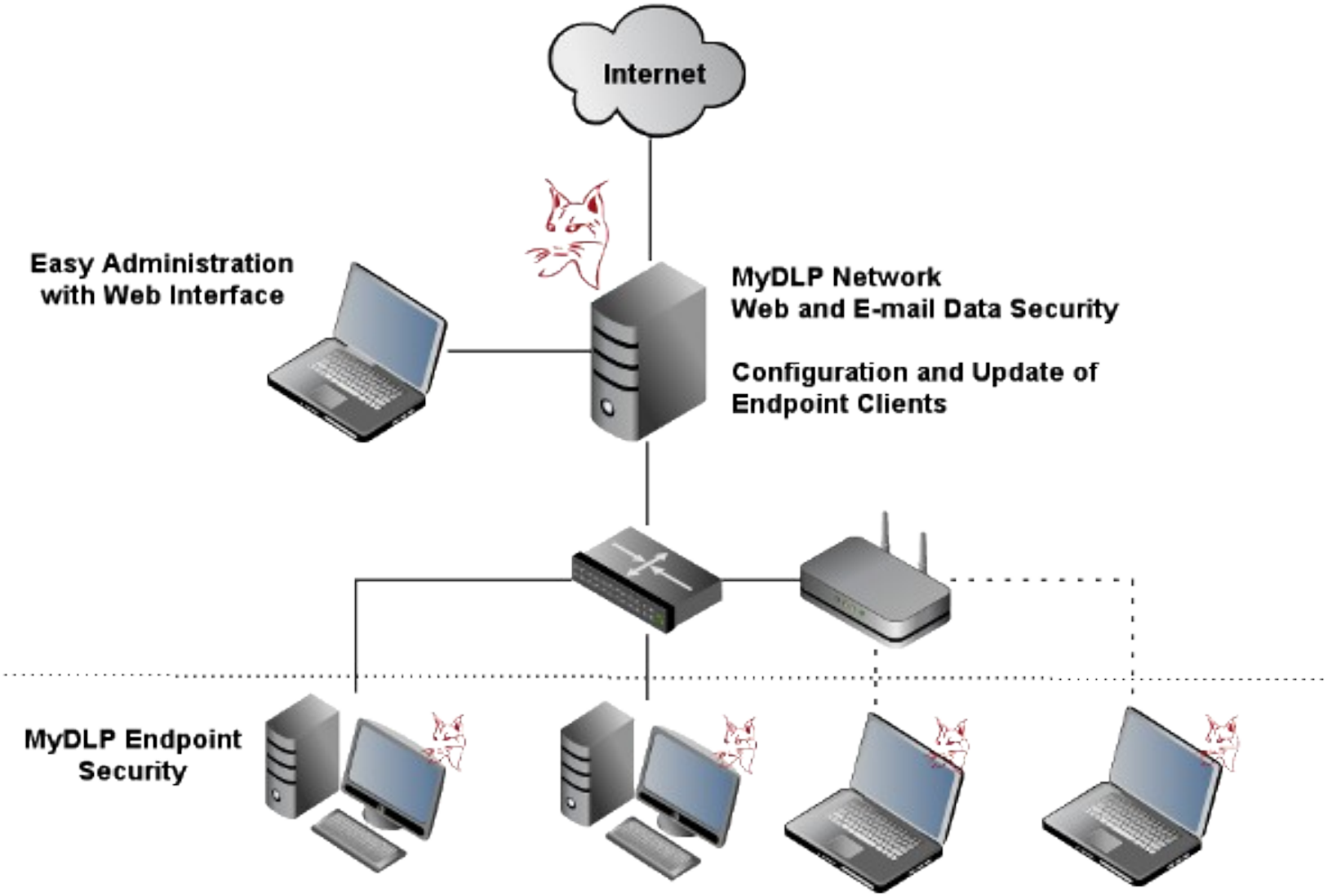
- Türkçe ve diğer Türki diller üzerinde istatistiki analiz.
- TC Kimlik No, kredi kartı gibi birçok öntanımlı veri tipleri.
- Detaylı olay takibi
- Geniş dosya formatı desteği
- Sunucular için bilgi güvenliği / ModDLP.
- HTTP (ICAP ile), SMTP (doğrudan Postfix veya SMTP Gateway olarak), USB, Printer, CD/DVD

- **MyDLP özelleştirilebilir.**
- **Amaç iş süreçlerini yavaşlatmadan bilgi sızıntısını engellemek.**

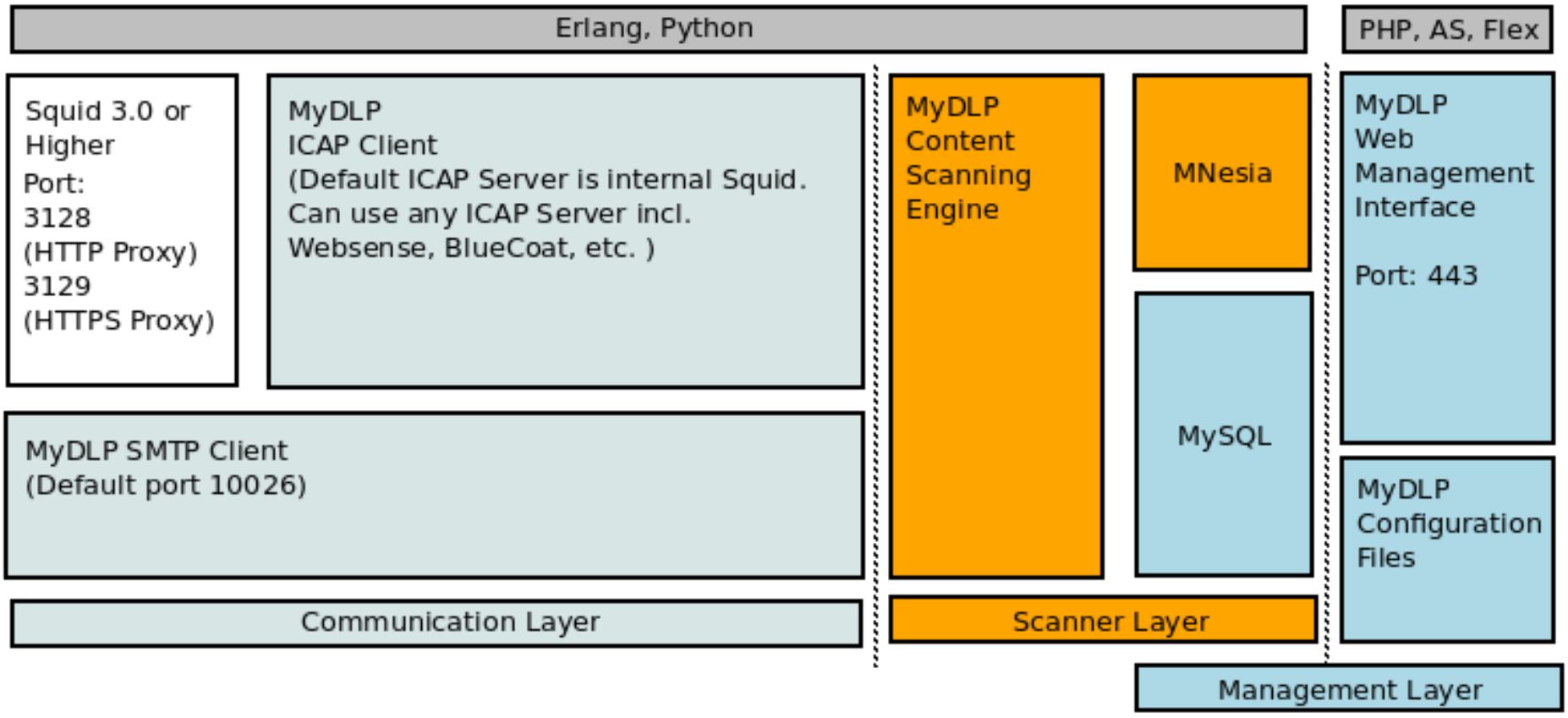
MyDLP Bileşenler

- **MyDLP Security Management:** İş süreçleri ile uyumlu politikalar oluşturarak gizli bilgi akışına dair kontrolleri tanımlar ve bu kontroller dâhilinde olayları raporlar.
- **MyDLP Security Monitor:** Kimin hangi gizli veriyi nasıl kullandığını izler.
- **MyDLP Network Security:** Ağda akan veriyi iş süreçlerine entegre politika-tabanlı kontroller ile korur.
- **MyDLP Endpoint Security:** Bilgi güvenliğini kontrollerini, entegre yönetim ve raporlama ile, uçbirimlere kadar genişletir.
- **MyDLP Web Security:** Web sunucunuz üzerinden dışarıya gizli veri çıkışını engeller.

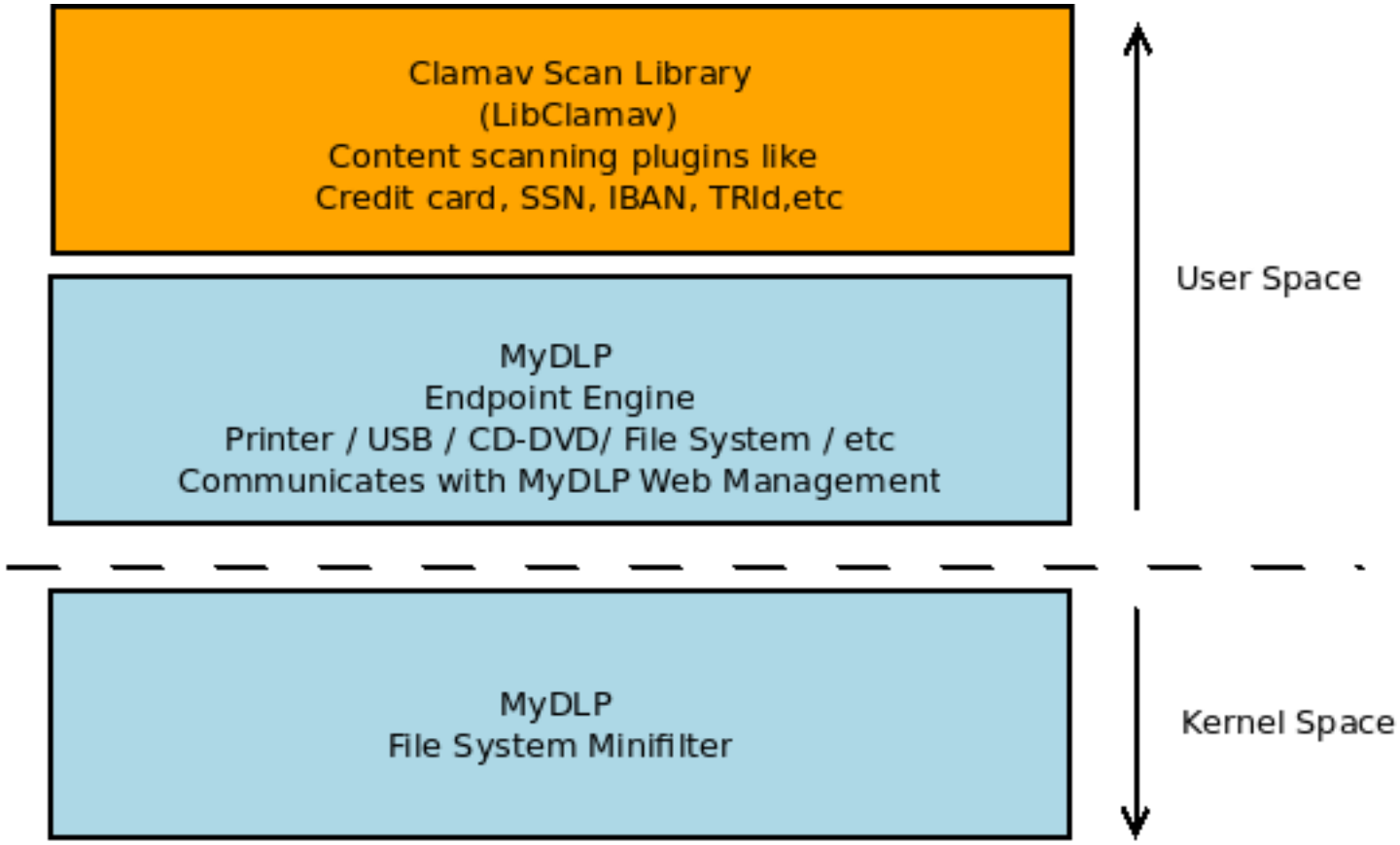
MyDLP Yapısı



Sunucu Mimarisi



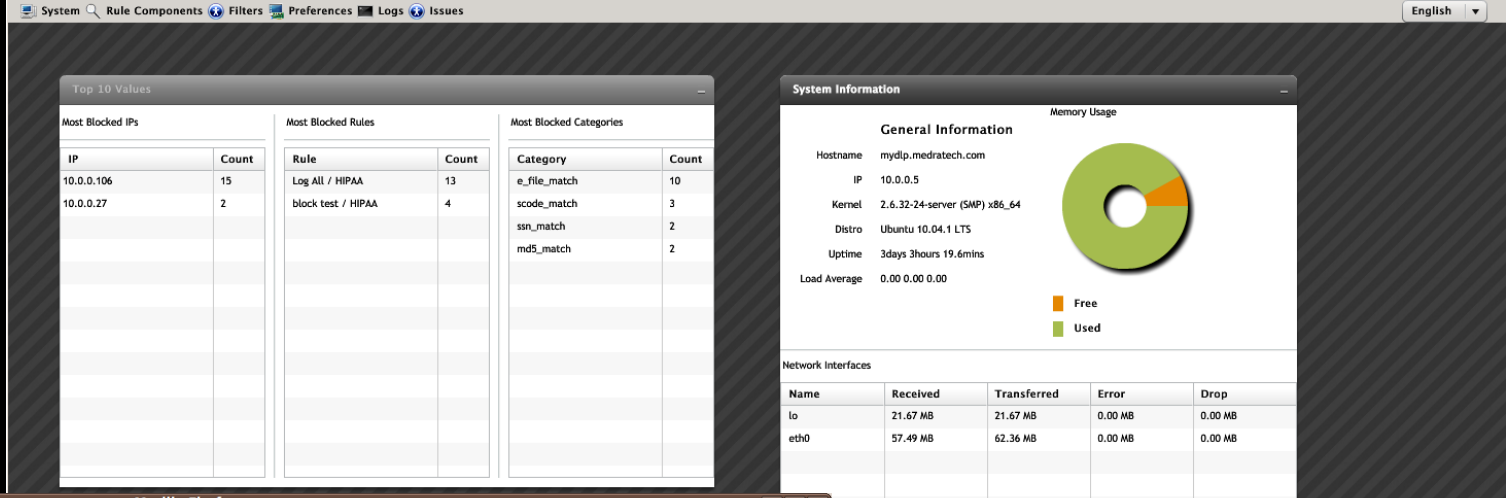
İstemci Mimarisi

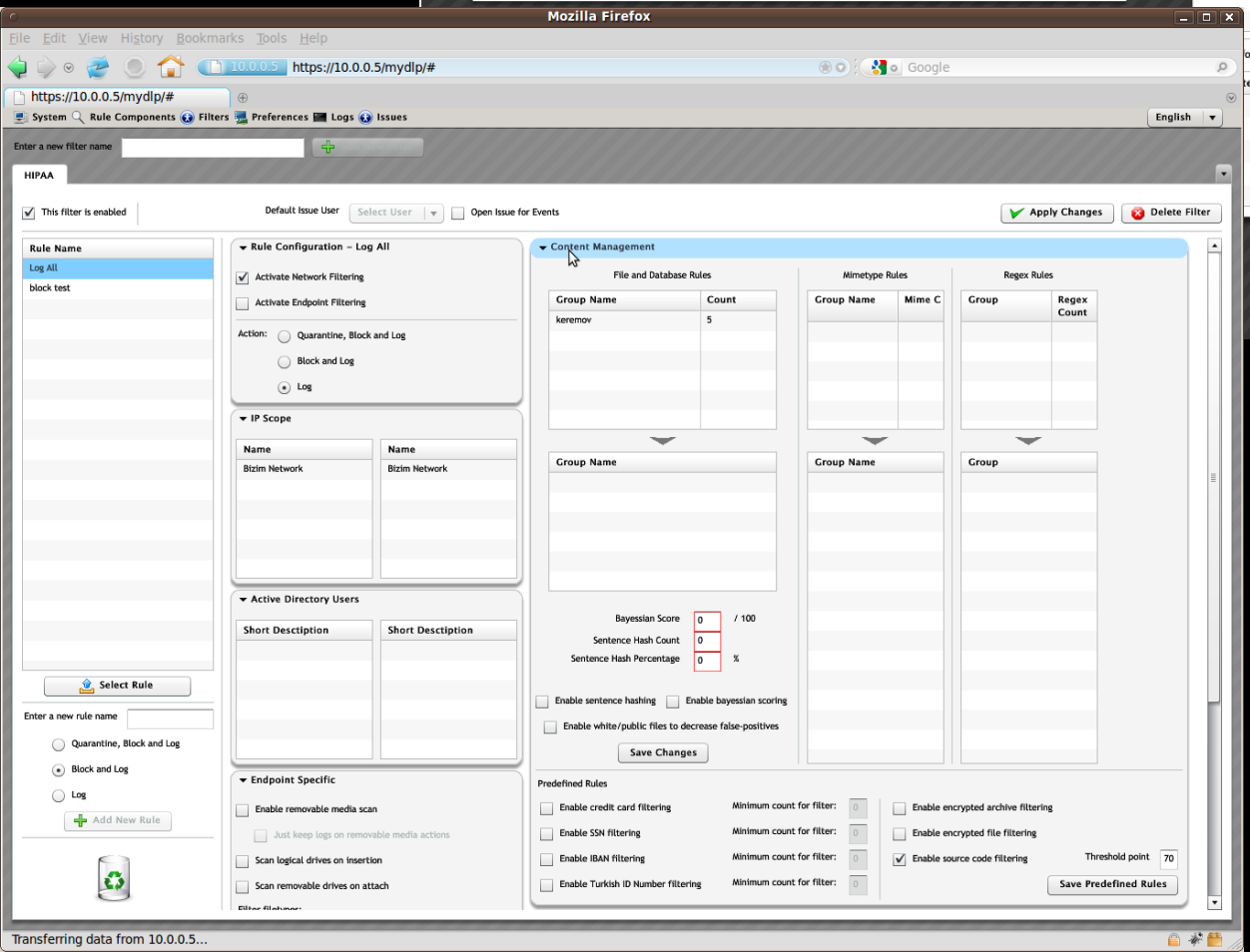


Ufak bir demo…

- MyDLP sanal makinesi üzerinde
  - MyDLP durumunun denetlenmesi
  - Temel ayarlar
  - Gizli veri tanımlamaları
  - Internet üzerinden dosyalar ve GET/POST isteklerinde filtreleme
  - Olayların incelenmesi

kim gizli bilgiye ulaşabilir?

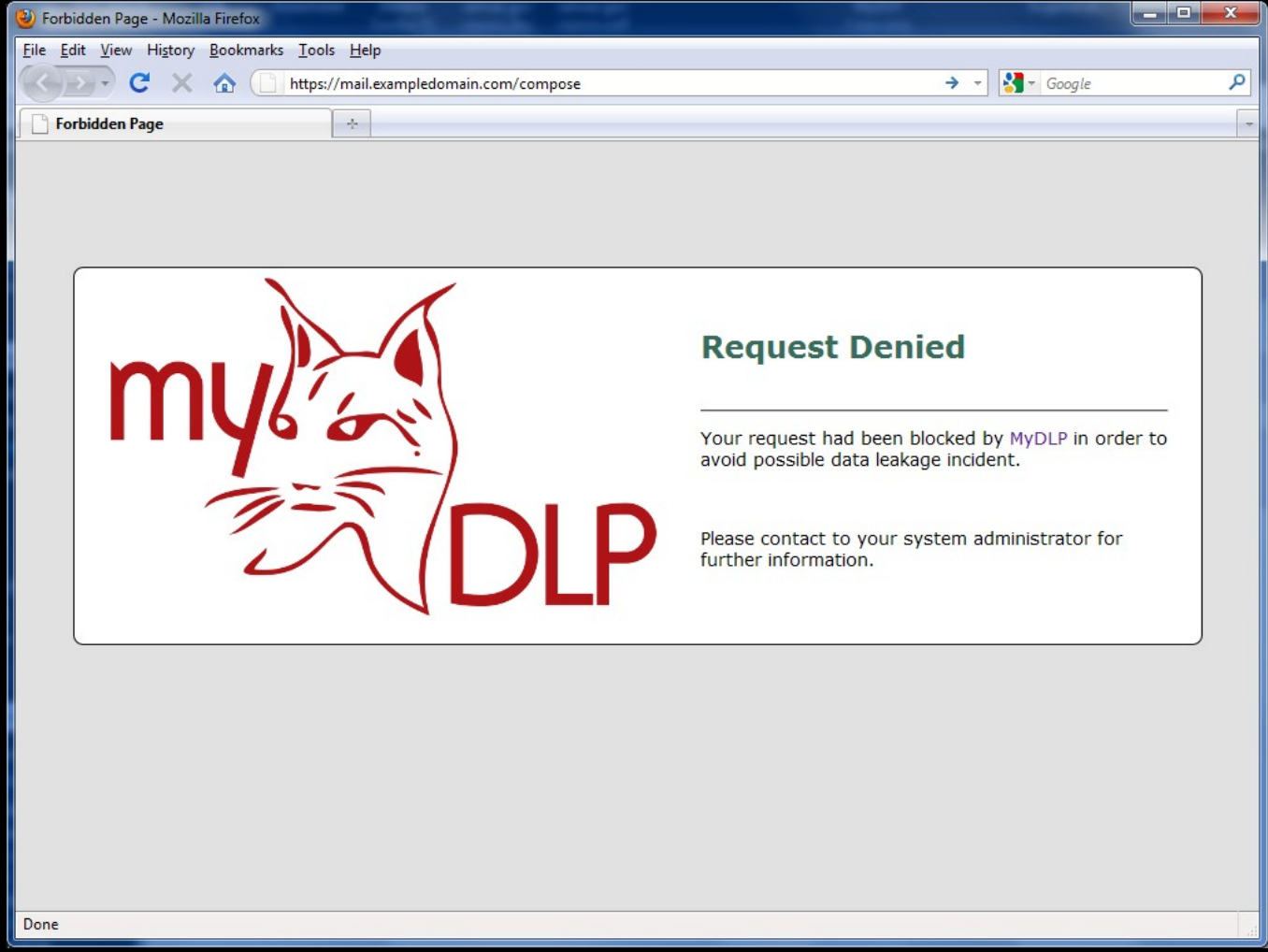




kim
hangi bilgiyi
hangi yollarla
nereden
nereye

taşıyabilir?

MyDLP veri akışı sırasında taşınan bilginin gizli olup olmadığını otomatik olarak tespit eder…



…ve **bilgi sızıntısı**nı engeller.

MyDLP Hakkında

BURAK OĞUZ, H. KEREM CEVAHİR & H. ÖZGÜR BATUR

MEDRA Teknoloji

Kurucular

DEVLERE KAFA TUTUYOR

Burak Oğuz ve H. Kerem Cevahir uzun yıllar boyunca özel sektörde pek çok açık kaynaklı projenin geliştirilmesinde rol aldılar. 2009 yılının Kasım ayında bilgi güvenliği alanında faaliyet göstermek üzere Medra Teknoloji'yi kurdular. 2010'da çekirdek ekiplerine H. Özgür Batur'u kattılar. MyDLP adını verdikleri çözümleriyle dünyanın ilk açık kaynaklı veri sızıntı önleme yazılımını kullanıma açtılar. 2010 yılının son çeyreğinde veri sızıntıları gibi konular gündemin önemli bir konusu haline gelince myDLP büyük bir ile karşı karşıya kaldı. 2011hedefleri ise bilgi güvenliği açısından bölgenin lideri konumuna gelmek... Görünen o ki bunu başaracaklar.

Bilgi sızdırmaya Türk çözümü

ODTÜ Teknokent'te faaliyet gösteren bir firmada görevli genç Türk mühendisler, internet üzerinden bilgi sızıntısını kaynağından engelleyen bir teknoloji geliştirdi. 'MyDLP' adlı yazılım, sızdırılan bilgileri yoğun bir erişim olduğunda kayıt altına alıyor ve yetkilileri anında uyararak bilgi aktarımını bloke ediyor. Genç mühendisler, 'Wikileaks' belgelerinin ortaya çıkmasıyla tarihinin en büyük bilgi sızıntısıyla karşı karşıya olan ABD'den sistem için yoğun talep alıyor. ODTÜ Teknokent bünyesinde faaliyet gösteren MEDRA firmasında görev yapan güvenlik ve yazılım mühendisi Hüseyin Kerem Cevahir, 'Wikileaks' belgelerinin dünyanın en büyük bilgi sızıntısı olduğunu belirterek, olayın veri aktarımını kaynağından engellemenin önemini ortaya çıkardığını söyledi. 'Wikileaks' olayından yıllar önce ODTÜ Teknokent, Sanayi Bakanlığı KOSGEB VE TÜBİTAK'ın desteğiyle internette bilgi sızıntısını engelleyecek 'MyDLP' adını verdikleri bir yazılım geliştirdiklerini anlatan Cevahir, yurt içinden ve dışından sisteme büyük ilgi olduğunu belirtti. 'MyDLP' projesinin tamamlandığını, ve yazılımın herkesin kullanabileceği şekilde 'www.mydlp.org' sitesinden dağıtılmaya başlandığını, konuyla ilgili ayrıntılı bilgiye bu siteden ulaşılabileceğini kaydeden Cevahir, uzmanlık gerektiren bu projenin hazırlık aşamasının uzun yıllar aldığını vurguladı. Cevahir, "Ürünümüz, kurumun bilgilerini tanıyor. Bu bilgi o kurum için gizli mi, değil mi buna karar verebiliyor. Ayrıca bilginin dışarıya sızmasını engelliyor" dedi.

Sorular ve Yorumlar

Katkılarınızı bekliyoruz…

Web: http://www.mydlp.org
E-Posta: mydlp@mydlp.org

Referanslar

- Oguz B.,Cevahir K.H., BT Yönetiminde Bilgi Sızıntısı ve Ağ Tabanlı Çoklu Protokol Bilgi Sızıntısı Engelleme, 3. ABGS Ankara, 2010
- Oltsik J., McKnight J., Gahm J., Protecting Confidential Data Revisited, ESG, Nisan 2009
- DLP Experts, Data Loss Monster: Beware The Pitfalls of DLP Deployment, http://www.dlpexperts.com