만료된 도메인의 전자우편을 통한 개인정보 유출에 관한 연구

김동현[1] · 홍윤석[2*]

[1]현대고등학교· [2]고양일고등학교

A Study on Privacy Violation Vulnerability Through E-Mail Sent to Expired Domains

DongHyun Kim[1] · YunSeok Hong[2*]

[1]Hyundai Senior High School · [2]Goyang il High School

E-mail : me@leok.kr / me@yunseok.kr

요 약

인터넷이 발전함에 따라 많은 사람들이 이메일로 문서를 주고 받거나 온라인 서비스에 가입하는 등 전자우편 사용이 증가하고 있다. 상용 이메일 서비스를 통해 제공되는 도메인을 사용하지 않고, 개인이나 교육기관의 자체 도메인을 사용하는 사례도 함께 증가하고 있다. 하지만 사용하던 전자우편의 도메인이 만료될 경우 다른 개인이나 기관이 해당 도메인을 사용 할 수 있고, 새로운 도메인 소유자는 도메인으로 전송되는 모든 전자우편을 수발신 할 수 있어 개인정보 유출 우려가 크다. 기존 이메일 주소로 전송되는 모든 전자우편을 확인할 수 있기에 비밀번호 재설정 안내, 신용카드 명세서, 전자상거래 주문 내역 등 민감한 개인정보를 포함한 전자우편 역시 열람할 수 있는 것이다. 본 논문에서는 외부 사이트 등 의존성이 유지된 채 전자우편로 사용되던 도메인이 만료될 때 야기되는 개인정보 피해를 기술하고 해결책을 제안하고자 한다.

ABSTRACT

With internet development, many peoples use their email to exchange documents, register for web services, and much more. Some individuals/organizations (including educational institutions) use their own domain name for email instead of a domain provided by commercial email services. However, suppose the domain used for custom email expires. In that case, other individuals/organizations can reuse the domain, and the new domain owner can send and receive all emails incoming to the domain. It makes us concerned about Privacy violations. Email that new domain owners can look into also contains sensitive emails like password reset notifications, credit card statements, order history, and more. In this research, we would like to describe the privacy violations caused by the expired domain used for email that did not remove all dependencies of email users and propose a solution.

키워드

이메일(Email), 도메인(Domain), 개인정보 유출(Privacy Violation)

Ⅰ. 서 론

본 논문에서는 만료된 도메인의 전자우편을 통한 개인정보 유출에 관해 서술한다. 상용 메일 서비스를 통해 제공되는 도메인을 사용하지 않고, 개인이나 교육기관의 자체 도메인을 사용하는 사례가 증가하고 있으며, 사용하던 전자우편의 도메인이 만료될 경우 다른 개인이나 기관이 해당 도메인을 사용할 수 있다. 새로운 도메인 소유자는 도메인으로 전송되는 모든 전자우편을 수발신할 수 있다는 점에서 발생할 수 있는 개인정보 유출 우려에 관해 기술한다.

* corresponding author

Ⅱ. 전자우편

1. 전자우편의 구성

전자우편은 “user@example.com”와 같은 형식으

로 이루어져 있으며 user와 example.com로 나뉘어 구성되어 있다. 이는 example.com 도메인에 속해있는 uesr에게 전자우편을 전송하는 것임을 이야기한다. 보내는 메일서버에서 example.com의 메일서버로 전송하여, example.com의 메일서버가 실 수신자인 user에게 메일을 보여주게 된다. 이 과정에서 보내는 메일 서버는 수신하는 메일 서버의 DNS MX Record를 조회하는 등의 과정을 필요로 한다.

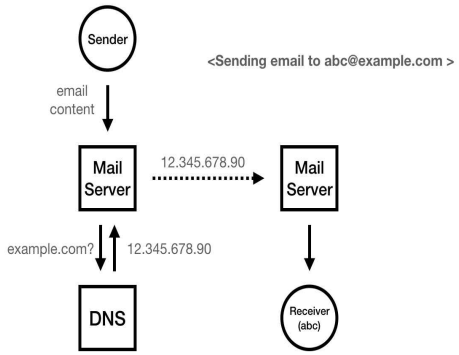

그림 1. 전자우편 전송 과정 흐름도

2. 위 방식의 특징

전화번호, 우편 등 여타 매체들과 다르게 최종 수신자에게 이메일이 직접 전달되는 방식이 아닌, 이메일이 도메인의 메일서버로 전달되고 해당 메일 서버에서 사용자에게 이메일을 보여주고 있다. 이에, 이용자는 자신의 의지와 관련없이 전자우편함의 변경이나 상실을 겪을 수 있으며, 이에 대한 통제권을 가지고 있지 않다. 예시를 들어, 전화번호나 우편의 경우 자신이 직접 전화번호를 변경하거나 주소지를 변경하였기에 해당 전화번호/우편으로 수신되는 연락을 정정해야 한다고 생각할 수 있지만, 이메일의 경우 사용자가 인지하지 못한 채 전자우편의 수신 대상이 변경될 수 있는 것이다.

III. 도메인

1. 도메인의 소유자가 변경될 수 있는 케이스

기관/기업이 파산 혹은 합병됨에 따라 기존 도메인의 기간이 연장되지 않는 경우, 원래의 소유자가 아닌 다른 사용자가 도메인을 소유할 수 있다. 또한 개인 도메인 소유자의 경우에도 동일하게 만료일로부터 일정 시간이 지날 경우 3자가 도메인을 소유할 수 있다.

2. 도메인의 새 소유자가 DNS 변경

변경된 도메인 소유자는 도메인을 구매하여 DNS 정보를 관리할 수 있게 된다. 이 때 DNS 정보로 이메일 수발신과 관련된 TXT, MX 레코드를 등록하여 해당 도메인으로 수신되는 이메일을 자신의 메일서버로 전송하여 전자우편을 이용할 수 있다.

IV. 만료된 도메인 의존성으로 인한 개인정보 유출

1. 전자우편의 만료된 도메인 의존성

앞서 언급한 것 과 같이 도메인의 소유주가 변경된다면 전자우편함 사용자의 의지와 관련없이 해당 도메인으로 전송되는 모든 이메일이 새로운 도메인 소유주에게 전송되게 된다. 본래 전송되어야 하는 기관/단체/개인이 아닌 제3자에게 이메일이 전송될 경우 후술하는 개인정보 유출 문제가 발생할 수 있다.

2. 신용카드 명세서 등 민감한 개인정보 유출

전자우편을 통해 일상생활에서 주로 사용하는 인터넷 쇼핑몰부터 시작해서 신용카드사까지 주문 내역, 청구서 등 다양한 정보를 주고받는다. 만료된 도메인의 의존성으로 인해 카드 사용 내역, 온라인 쇼핑몰 주문 내역 등 민감한 개인정보 유출될 수 있다.

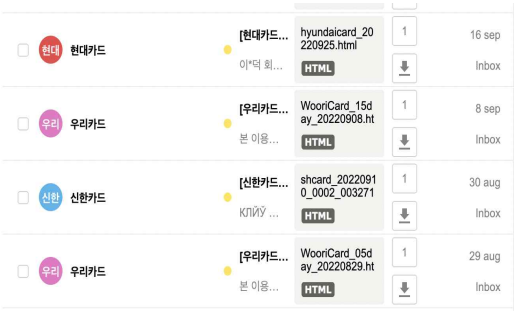

그림 2. 신용카드 명세서

2. 비밀번호 초기화 기능을 통한 유출

유명 N 사 혹은 K 사 등 다양한 포털 사이트 및 전자상거래 사이트, SNS 등에서는 “백업 이메일”을 지정할 수 있도록 되어있고, 이메일 인증을 통해 아이디 및 비밀번호를 찾아 계정에 접근할 수 있도록 구성 되어있다. 이 경우, 단순히 이메일로 수신되는 정보 뿐만 아니라 해당 이메일을 백업 이메일로 사용하는 모든 온라인 사이트 계정에 직접적인 접근권한을 얻게되어 심각한 개인정보 유출 및 명의도용 등 다양한 피해를 초래할 수 있다.

그림 3. “비밀번호 찾기” 페이지

3. 테스트 결과

국내 기관인 K사가 타 기관에 흡수 합병됨에 따라 기존에 전자우편으로 사용했었던 도메인의 유지관리가 되지 않았다. 해당 도메인은 만료일이 도래해 자동으로 만료되어 도메인 시장에 공개되었고, 본 연구를 진행하기 위해 연구진은 해당 도메인을 구입하여 수신되는 이메일을 확인하였다.

약 1년동안 수신되는 전자메일을 수집한 결과, 약 3만건의 전자우편을 수신하였다. 수신한 전자우편 중 신용카드 명세서, SNS 채팅 알림, 온라인 쇼핑몰 결제/배송 알림 등 민감한 내용을 포함 할 수 있는 전자우편이 포함되어 있었다.

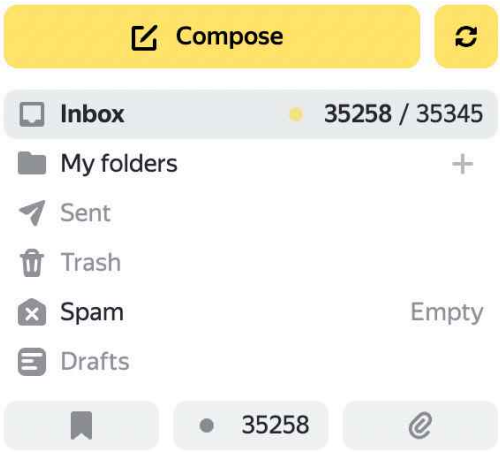

그림 3. 전자우편 “Inbox”

Ⅴ. 해결 방안

1. Whois 정보 Created_at 기반 대응

도메인 등록 기관에서 제공하는 Whois 정보에는 도메인이 등록된 날짜를 의미하는 Create_at 레코드가 있다. 도메인이 만료되어 새로운 소유자가 도메인을 다시 구입할 경우, 도메인이 등록된 날짜를 의미하는 created_at 레코드가 변경될 것이다. 도메인 등록 날짜를 기반으로 기존에 전송하던, 의도된 수신자에게 도달되는 것인지 확인 절차를 걸친다면, 보안을 유지할 수 있다.

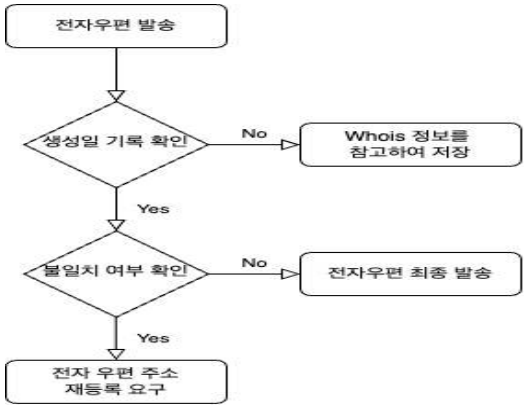

그림 4. Whois 생성일 기반 검증 흐름도

Whois 생성일 기반 검증의 예시를 들면, 백업 이메일로 등록되어 있는 이메일 주소로 이메일을 전송할 때 마다 Whois의 Created_at 레코드를 저장해 둔다. 추후 해당 주소로 이메일을 전송할 때 이전에 저장해둔 값과 현재 Created_at 레코드 일치 여부를 확인한다. 직전에 전송했을때와 현재의 Created_at 정보를 비교하여 변경되었다면 도메인의 소유자가 변경된 것으로 판단해 이메일을 전송하지 않고 보류해 두고 사용자에게 타 연락수단으로 이메일 주소 재등록을 요구하는 것이다.

2. P2P 암호화 기반 대응

PGP나 S/MIME등 이미 기업들에서는 자주 사용하는 P2P 암호화를 개인에게 전송되는 이메일 에도 적용하는 등 더 넓은 범위에 적용하여, 민감한 개인정보를 담고있는 이메일을 전송할 때 상대방의 공개 키로 암호화 하여 전달하는등 내용을 P2P 암호화하여 전달 할 경우 도메인의 소유주가 바뀌어 제3자에게 이메일이 전송되어도 개인정보 유출 문제를 줄일 수 있다.

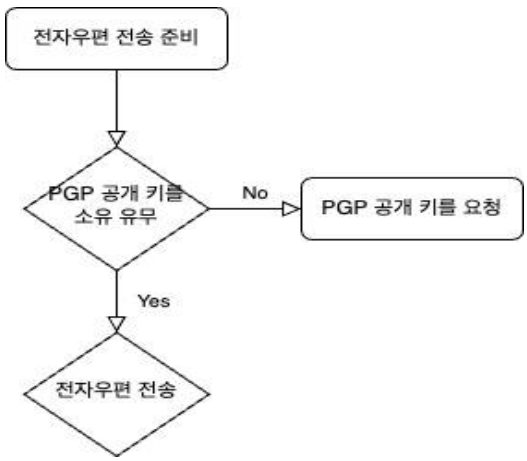

그림 5. PGP 암호화를 통한 전자우편 발송 흐름도

Ⅴ. 결 론

현재 전자우편 시스템은 만료된 도메인에 대한 의존성으로 인해 생길 수 있는 개인정보 침해 문제를 고려하지 않고 있다. 본 논문에서는 도메인이 만료됨에 따라 발생하는 이메일을 통한 개인정보 침해 문제를 발견하고 해결 방안을 제시하여 기업/기관이 개인정보 침해 문제를 줄이고 보안성이 더 강화된 믿을 수 있는 전자우편 시스템을 구축하여 상용화되기를 희망하며 논문을 마친다.

References

[1] F. A. Maqbali and C. J. Mitchell, “Email-based Password Recovery - Risking or Rescuing Users?,” *2018 International Carnahan Conference on Security Technology (ICCST)*, 2018, pp. 1-5, doi: 10.1109/CCST.2018.8585576.

[2] G. Liyange and S. Fernando, “A comprehensive secure email transfer model,” *2017 IEEE International Conference on Industrial and Information Systems (ICIIS),* 2017, pp, 1-5, doi: 10.1109/ICIINFS.2017.8300341

[3] D. Kuobin, “PGP E-mail Protocol Security Analysis and Improvement Program,” *2011 International Conference on Intelligence Science and Information Engineering*, 2011, pp. 45-48, doi: 10.1109/ISIE. 2011.144.

[4] J. Ruohonen, “Measuring Basic Load-Balancing and Fail-Over Setups for Email Delivery via DNS MX Records,” *2020 IFIP Networking Conference (Networking)*, 2020, pp. 815-820.