북한개발소식 03

2021 March | 통권 185호

| 이달의 주제 |

북한의 사이버 위협과 선교 보안

한국오픈도어 북한선교연구소

CONTENTS

2021 March

이달의 주제 :

북한의 사이버 위협과 선교 보안

+ Foreword

권두칼럼

북한의 사이버 위협과 선교 보안

오픈도어선교회 북한선교연구소

최근 수년간 북한발 해킹에 대한 다양한 기사들이 나오고 있다. 국내 굴지의 기업들과 정부 부처와 기관, 국회의원에서부터 해외 단체들과 기업에 이르기까지 북한은 전 세계를 무대로 해킹을 자행하고 있다. 미국의 FBI 같은 주요 정보기관과 IT보안 관련 기업들은 최근 북한이 각종 해킹의 주요 행위자가 되었음을 계속 강조하며 지속적으로 경고하고 있다. 하지만 일반 교회와 성도들에게는 경제 상황이 열악하고 기술이 상대적으로 뒤떨어지는 북한이 이렇게 광범위하게 해킹을 한다는 것이 피부에 잘 와 닿지 않는 일인 듯하다. 그러다 보니 상대적으로 북한의 사이버 위협에 대해서 별 생각이 없거나 심지어는 사건사고의 책임을 만만한 북한 탓으로 돌리는 것 아니냐는 의문을 가지기도 한다.

우리의 부족한 인식과는 별개로 현장에서 느끼는 사이버 위협은 심각한 수준이다. 국내외를 막론하고 북한이 불편해할만한 활동을 전개하는 기관 및 단체는 모두 이러한 위협에 노출되어 있다. 실제로 이메일이 해킹당하거나 각종 해킹 툴을 통해 자료가 유출되는 사례는 이미 빈번하게 보도되고 있으며 기사화, 공론화 되지 않은 북한의 사이버 공격도 상당수이다. 정보의 디지털화와 스마트폰의 발달 등의 시대적 흐름 속에 사이버 공격의 위험성도 더욱 커지고 있다. 무엇보다 보안이 중요한 북한 선교 현장에서 이러한 사이버 위협은 신변을 보호받아야 할 주요 선교사 및 선교동역자를 노출시

키고 심각한 위협에 빠뜨리게 하고 있다.

특히 안타까운 점은 이러한 해킹 공격으로 인한 피해가 국내에서도 다수 발생하고 있다는 사실이다. 선교지에서는 극도의 보안을 지키고자 애쓰는데 정작 상대적으로 안전하고 조금만 노력하면 사고를 예방할 수 있는 국내에서 사건이 발생하고 있다는 사실은 우리의 부주의에 대한 반성을 촉구한다.

이번 글에서는 최근 북한 관련 사이버 위협의 실태를 중심으로 우리의 대응과 기도의 제목을 나눠보고자 한다.

북한 사이버 위협 실태와 북한선교

아마 북한의 해킹이 언론의 주목을 받은 계기는 2014년에 있었던 소니 픽처스 해킹일 것이다. 북한 지도자 암살을 내용으로 한 코미디 영화 “더 인터뷰” 와 관련하여 북한의 소행으로 추정되는 해킹 공격이 있었다. 회사 관계자 간 개인 메일, 직원의 개인 정보, 미공개 영화 본편의 복사 등 다양한 정보가 유출되었다. 비록 북한 측에서는 자신의 소행이 아니라고 주장했지만 당시 오바마 행정부는 북한의 소행으로 보고 공식적으로 사이버 보복을 실시했다. 18년 9월에는 미 법무부에서 소니 픽처스 해킹을 포함하여 2016년 방글라데시 중앙은행 해킹, 2017년 워너크라이 랜섬웨어 해킹의 배후로 북한 국적 해커 박진혁 씨와 그가 속한 회사를 제재 명단에 올리고 기소하기도 했다. 소니픽처스 해킹 사건은 한 국가가 민간 기업을 상대로 저지른 충격적인 사례로 사이버 보안 업계에서 통용되고 있다.[1]

최근에도 북한의 해킹이 언론의 관심을 모았다. 백신 관련 제약사들을 해킹한 정황이 보도된 것이다. 월스트리트저널은 북한이 국내외 제약사 6곳에 해킹을 시도했다고 밝혔다. 로이터 통신도 3곳을 더해 9곳이 공격을 받았다고 보도했다. 코로나19로 인한 감염자가 ‘0’명이라고 주장해온 북한이기에 북한의 제약사 해킹은 더욱 관심을 받았다.[2] 북한의 해킹 공격은 계속해서 진화하여 2014년 소니 픽처스 해킹 당시만 하더라도 그저 표적을 파괴하는데 목적을 둔 공격이었다면 이제는 원하는 대상에게 피해를 입히는 것을 넘어서 돈을 목적으로 금융 조직을 공격하고 있다.[3] 16년 방글라데시 중앙은행 해킹을 비롯하여 ATM 해킹에서부터 암호화폐 거래소 해킹까지 북한의 해킹 표적은 계속 확대되고 있다.

〈김정은 암살을 소재로 다룬 영화 '더 인터뷰'〉

북한은 전 세계를 대상으로 해킹을 시도하고 있지만 그 주요 표적은 단연 한국이다. 19년 유엔의 대북제재위원회 보고서에 따르면 북한이 사이버 해킹으로 20억 달러를 탈취했으며, 이 중 한국이 10건으로 가장 많이 피해를 입었다. 한국의 구체적인 피해 금액은 알려지지 않았지만 제재위가 북한 소행으로 추정되는 17개국 최소 35건의 해킹을 조사 중이라고 밝혀 한국의 피해 사례가 3분의 1에 달할 것으로 추정된다.[4]

물론 한국에 대한 사이버 공격은 단순히 피해액으로만 계산할 수 없다. 북한의 남한에 대한 해킹은 당연히 정보 탈취의 목적이 중요하기 때문이다. 북한은 정보 획득을 위한 해킹시도를 다수 시도해왔다. 1차 미·북 정상회담이 열릴 무렵 청와대 국가안보실을 사칭한 위장 메일이 발견됐고, 2019년 1월에는 통일부 기자단 77명에게 악성 메일이 일괄 발송됐다. 2019년 2월 2차 미·북 정상회담을

최근에도 북한의 해킹이 언론의 관심을 모았다. 백신 관련 제약사들을 해킹한 정황이 보도된 것이다. 월스트리트저널은 북한이 국내외 제약사 6곳에 해킹을 시도했다고 밝혔다.

1 “소니를 완전히 불태워버렸다…北 해킹능력 세계 톱5 수준”, 중앙일보, 2019.02.09., 〈https://news.joins.com/article/23356051〉(검색일: 21. 02. 15)

2 “백신·치료제 해킹 시도…범인은 북한 ‘김수키’?”, MBC, 2020.12.03., 〈https://imnews.imbc.com/replay/2020/nwdesk/article/6008549_32524.html〉(검색일: 21.02.15)

3 “수년 만에 세계적 위협이 된 북한, 앞으로 어떻게 변할까?”, 보안뉴스, 2020.12.02 〈https://www.boannews.com/media/view.asp?idx=93093〉(검색일: 21.02.15)

4 "北, 해킹으로 20억弗 탈취…한국이 최대 피해", 한국경제, 2019.08.13 〈https://www.hankyung.com/politics/article/2019081326551〉(검색일: 21.02.15)

〈18년 12월, 경북 하나센터의 PC가 해킹당해 탈북민 997명의 신상이 유출되었다. 사진은 사건 관련 하나센터의 공지사항 캡처 (데일리 NK)〉

앞두고도 '미·북회담 특별좌담회 초청장'(2월 21일)을 빙자한 악성 메일이 발견됐다. 탈북민에 대한 정보탈취도 극성이다. 2018년 12월에는 탈북민 997명의 신상정보 유출이 확인됐다.[5]

북한의 해킹은 시간이 갈수록 점점 더 심해지고 있다. 작년(2020년)에 발생한 사례들만 살펴보아도 다수의 해킹 시도가 있었다. 탈북민 출신 태영호 의원에 대한 스마트폰 해킹[6]과 지성호 의원 사무실 이메일 대상으로 한 해킹[7] 시도가 있었다. 북한인권위원회 (HRNK) 등의 외국계 북한 인권 단체[8]들을 비롯하여 통일부 북한인권정보센터에 대한 해킹 시도도 포착되었다.[9] 국내 북한 관련 단체나 활동가들에 대한 공격도 다수 포착되었다.

이러한 북한발 해킹에 선교단체도 예외가 되지 않는다. 선교단체에 대한 북한의 해킹 시도 역시 확인되고 있다. 이러한 해킹 공격은 선교사와 현장 사역자의 안전에 큰 위협이 되고 있다. 북한 사역에 참여하는 선교사가 주로 머물고 있는 제 3국의 보안 상황은 이미 심각한 통제와 감시가 이루어지고 있다는 점은 익히 잘 알려진 사실이다. 특히 중국의 경우 2017년 사드사태를 기점으로 시작된 선교사 추방 사태를 통해 중국 내 선교사들의 정보가 인지하지 못한 가운데 유출된 것을 뼈저리게 경험할 수 있었다. 당시 중국은 이미 선교사의 파송 단체나 선교사 파송장 등 관련 정보를 확보한 상태에서 선교사들의 집을 압수수색하고 연행하여 조사하였다고 선교사들은 증언한다.[10] 이미 상당한 정보가 유출된 것이다. 17년 2월에 열린 위기관리포럼에서 당시 경험을 증언한 한 선교사는 온라인 해킹에 대한 정황과 우려를 언급하기도 하였다.[11] 이미 선교현장에서 사이버 위협은 심각한 수준인 것이다. 이런 가운데 북한의 소행으로 의심되는 해킹까지 갈수록 증가하는 추세는 선교사와 사역자들에 대한 사이버 공격이 위험수위에 이르렀음을 보여준다.

해킹으로 인한 피해는 단순히 해외에 체류해야 하는 선교사에게만 국한되지 않는다. 앞서 언급한 사례에서 보듯이 국내 거주 탈북자들의 정보는 북한 내에 남아있는 친인척의 신변을 위협할 뿐 아니라 역으로 협박의 용도로도 활용될 수 있다. 특히 북한 선교에 직간접적으로 참여하고 있는 탈북자 및 조선족들의 신원이 노출된다면 안전은 물론이고 사역 전반이 위험에 처할 것이라는 사실은 자명하다.

파송국 보안의 중요성

이상 언급한 사례들과 최근의 경향을 통해 배울 수 있는 교훈은 선교사 파송국인 한국도 더 이상 보안 안전지대가 아니라는 사실이다. 북한개발소식에서는 그 동안 선교 현장에 체류하는 선교사들의 보안과 안전에 대해서 중점을 두고 소개해왔다. 선교사들의 보안 환경이 워낙 열악하기도 하고, 한국교회가 이에 대한 인식과 기도가 필요하다는 관점에서였다. 그렇지만 국내의 단체나 활동가들 개인에 대한 해킹 시도가 계속해서 증가하면서 이제 파송국인 한국에 위치한 교회와 단체들 역시 심각한 보안 위협에 맞닥뜨리고 있다.

이전부터 본국의 열악한 보안 의식으로 인한 선교 현장의 피해는

해킹으로 인한 피해는 단순히 해외에 체류해야 하는 선교사에게만 국한되지 않는다. 앞서 언급한 사례에서 보듯이 국내 거주 탈북자들의 정보는 북한 내에 남아있는 친인척의 신변을 위협할 뿐 아니라 역으로 협박의 용도로도 활용될 수 있다.

5 손영동, "북한의 대남 사이버 공격 실태와 사례", 월간 북한 19년 7월호, pp. 44-50.

6 北, 태영호 폰 해킹… 문자까지 털어갔다, 조선일보, 2020.02.17 〈https://www.chosun.com/site/data/html_dir/2020/02/17/2020021700095.html〉 (검색일: 21.02.16)

7 지성호 의원 "지난달 두 차례 해킹 당해", 자유아시아방송, 2020.12.08〈https://www.rfa.org/korean/in_focus/ne-yw-12082020104430.html〉 (검색일: 21.02.16)

8 "DC 북인권단체에 북한 추정 사이버 공격 잇따라 포착", 자유아시아방송, 2020.05.29 〈https://www.rfa.org/korean/in_focus/nkhacking-05292020160533.html〉 (검색일: 21.02.16)

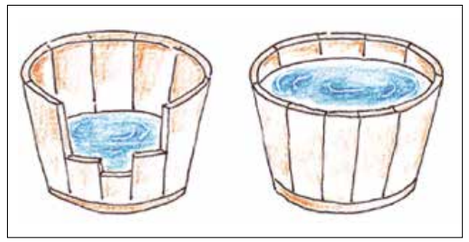
9 해킹그룹 탈륨, 통일부 북한인권기록센터 위장 공격, 시큐리티뉴스, 2020.10.16 〈https://www.boannews.com/media/view.asp?idx=91616〉 (검색일: 21.02.16)

10 "한국교회, 멀리 보고 중국교회와 동역 시대 열어가야", 크리스천 투데이, 2017.02.21 〈https://www.christiantoday.co.kr/news/297591〉 (검색일: 2021.02.16)

11 위의 글

종종 거론되어 왔다. 현장에 있는 선교사들은 이미 생활 속에서 보안 위협을 피부로 느끼기 때문에 아무래도 문자 하나 전화 한 통 쓰는 것도 조심하고 인터넷 사용에도 주의를 기울이는 것이 보통이다. 특히 최근 주요 선교지들은 창의적 접근지역으로서 선교사 채류나 선교활동을 허용하지 않는 곳이 다수인 관계로 파송된 선교사들은 선교사로서의 신분을 숨기고 생활하게 된다. 그렇지만 본국에서 날아오는 교회적 용어와 표현이 듬뿍 담긴 문자나 연락은 이러한 선교사의 노력을 허사로 만든다. 과거와 같이 보안을 위한 조치로 특정 용어를 자음만 사용하는 수준으로는 이미 선교 국가의 정보 감시를 피할 수 없다. 특히나 북한 선교와 연관된 인근 국가들은 언어적으로 큰 어려움 없이 관련 내용을 확인할 수 있는 능력이 충분한 만큼 더 큰 주의가 요망되는 지역이다.

이렇듯 선교 현지 뿐 아니라 파송국 후원 교회나 단체의 보안의식이 중요하지 않은 적이 없었지만 이제는 전보다 더 높은 수준의 보안 의식과 조치가 요구되고 있다. 먼저 기술의 발달로 모든 정보들이 전산화 되고 있으며, 이 내용들이 온라인을 통해 쉽게 전달되고 있다. 컴퓨터는 물론이고 스마트폰을 통해 다양한 업무 처리와 커뮤니케이션이 가능해지면서 이러한 도구들 없이 업무를 하는 상황을 상상하기 어려울 정도로 중요한 비중을 차지하게 되었다. 하지만 이러한 전산화, 온라인화는 해킹의 위협에는 매우 취약하다. 선교사는 신분을 잘 숨겼더라도 본국의 파송 단체나 후원 교회, 개인이 해킹을 당한다면 자연스럽게 선교사의 인적사항이나 연관된 현장 사역자 및 사역 관련 정보 유출로 이어지게 된다. 특히 최근 해킹 양상은 적극적인 조치를 요구한다. 과거에는 단체나 교회가 선교사의 기도편지를 홈페이지에 개시하거나 하는 식의 부주의와 실수로 인한 우발적인 유출이 많았다면 최근에는 직접적으로 단체의 대표 메일이나 주요 사역자를 겨냥한 피싱 메일 등을 통해 메일의 비밀번호를 가로채기도 하고 더 나아가 악성 코드가 담긴 첨부파일을 그럴듯한 문서 등으로 위장시켜 발송함으로서 인지하지 못한 가운데 컴퓨터가 감염되고 컴퓨터 내의 정보를 자동으로 전송하는 등의 직접적인 공격이 자행되고 있다. 스마트폰을 대상으로 한 해킹 문자나 톡을 통해 스마트폰의 문자 메시지나 주소록 등을 빼돌리는 해킹도 이루어지고 있다. 이러한 공격에 당장 내가 표적이 되지 않았다고 안도할 것이 아니라 어느 때라도 이런 공격을 당할 수 있다는 경각심을 가지고 미리 보안을 강화하기 위한 조치에 힘쓰는 것이 필요하다.



〈최소량의 법칙을 묘사한 삽화. 왼쪽과 오른쪽 항아리는 거의 비슷한 크기이지만 왼쪽 항아리의 일부 부분이 낮기 때문에 물을 담는 양에 차이가 발생한다. 즉 항아리의 최소인 부분이 항아리의 용량을 결정한다.〉

독일의 화학자 유스투스 폰 리비히가 주창한 “최소량의 법칙” 이론이 있다. 식물의 성장을 좌우하는 것은 넘치는 영양소가 아니라 가장 부족한 영양소라는 이론이다. 다시 말해 제아무리 좋은 환경에 다른 영양소가 풍부하더라도 어떤 영양소가 최소한의 필요를 충족시키지 못하면 식물의 생육과 성장에 지장을 받을 수밖에 없다는 말이다. 이러한 최소량의 법칙은 생물 영역에만 국한되지 않는다. 보안 측면에서 보면 전반적인 보안 수준은 높더라도 그 중 한 두 사람 또는 기관의 보안 수준이 낮다면 전체의 보안수준 역시 낮다고 볼 수 있다. 현지의 선교사와 동역자, 그리고 본국에서 함께하는 단체 및 교회 등을 한 팀이라고 본다면 어느 한 쪽만 보안 의식이 높아서는 전체적인 보안 수준 향상을 기대할 수 없다. 특히 최근 보안 사고들을 살펴볼 때 본국의 IT 역량 수준과 밀접한 관련이 있는 것으로 알려져 있다.

이번 북한개발소식의 글들은 북한의 주로 사용하는 해킹 수법과 관련하여 사례와 대응 방안, 그리고 관련된 보안 의식 향상을 주제로 꾸려져있다. 이러한 자료를 바탕으로 시중의 관련 전문 자료들을 참고하여 예방/대응 시스템을 세울 필요가 있다. 무엇보다도 보안에서 가장 중요한 것은 구성원들의 보안 의식이라는 점에서 교육에도 노력을 기울여야 한다. 한국세계선교협의회(KWMA) 산하 한국선교평가원(KMES)에서 주기적으로 개최하는 선교보안세미나

컴퓨터는 물론이고 스마트폰을 통해 다양한 업무 처리와 커뮤니케이션이 가능해지면서 이러한 도구들 없이 업무를 하는 상황을 상상하기 어려울 정도로 중요한 비중을 차지하게 되었다. 하지만 이러한 전산화, 온라인화는 해킹의 위협에는 매우 취약하다.

를 비롯하여 FMnC 선교회 등 전문 기술을 가지고 봉사하는 선교회 등을 통해 교육을 비롯한 전반적인 선교 보안 향상에 도움을 받을 수 있다.

무엇보다 선교회의 보안 향상에는 전 조직적인 결단과 투자가 필수적이다. 보안의 향상은 기본적으로 불편과 어려움을 동반한다. 간단하게 처리할 수 있는 일을 더 복잡하게 단계를 거쳐야 하고, 별도의 비용을 들여야 하는 번거로운 일이다. 그러다보니 보안에 대해 중요하다고 말하지 않는 사람은 없지만 실제로 보안 향상을 위해 적극적으로 나서지 않게 되곤 한다. 특히 상대적으로 안전한 국내에서는 보안 의식이 소홀해지기 쉽다. 이러한 악순환을 끊기 위해서는 전 구성원의 결단과 투자가 필요하다.

사사기 7장에는 하나님께서 기드온과 함께 할 삼백 용사를 선발하시는 장면이 등장한다. 두려워하는 이들을 모두 돌려보내고도 아직 숫자가 많다고 하신 주님께서는 군대를 강가로 데리고 가 물을 마시게 하셨다. 그리고 헐레벌떡 강에 입을 대고 물을 마시는 이들은 돌려보내고 무릎 꿇고 손으로 떠 마시는 이들만 뽑아 사용하셨다. 이 구절은 군사의 자세에 대해 교훈을 주는 구절이라고 해석된다. 즉 군인으로서 전쟁을 앞두고 항상 경계하고 주의해야 함에도 불구하고 정신없이 시야를 확보하지 않고 강에 입을 대고 마신 부주의하고 깨어있지 않은 이들은 돌려보내신 반면 경계를 늦추지 않은 이들은 사용하셨다는 것이다. 어찌 보면 특별할 것 없는 물 마시는 일일 뿐이지만 그럼에도 항상 깨어있는 이들이 하나님께 쓰임받았다는 교훈을 생각할 때 선교에 참여하는 우리 역시 작은 일에도 항상 깨어 있으며 경계하는 자세를 가지는 것이 마땅할 것이다. 하나님의 지상명령에 충성하는 군인의 자세로 항상 깨어서 쓰임 받는 우리 모두가 되길 바라며 또 선교에 참여하는 이들을 위한 형제자매의 관심과 기도가 계속되길 기대한다.

칼럼_1 + Column

북한의 사이버 공격과 선교

오픈도어 현장 사역자

최근 들어 남한사회의 중요한 이슈들이 있을 때마다 이와 관련된 북한의 사이버 위협 이슈가 함께 등장하고 있다. 비트코인 열풍이 한창이던 2018년 이후로 북한정부와 연관된 것으로 추정되는 비트코인 거래소에 대한 해킹을 본격화 했다. 최근 보도에 의하면 북한은 2015년부터 2020년 9월까지 15억 달러 이상의 가상화폐를 탈취한 것으로 전해진다.[1] 최근 코로나19 백신과 치료제에 대한 전 세계의 관심이 집중된 가운데 북한에 의한 전 세계 제약사들에 대한 해킹시도 역시 드러나고 있다.

실제로 북한의 해커집단은 인터넷으로 연결된 세계의 모든 컴퓨터를 해킹의 대상으로 하고 있다. 북한의 사이버위협이 과거 정부기관을 목표로 했던 것에서 점차 민간기업과 사회단체 개인에게로 확대된 것은 잘 알려진 사실이다. 언제든지 세상에 새로운 사건이 발생한다면 북한의 해커집단은 그와 관련한 홈페이지를 휘저으며 새로운 먹잇감을 찾을 것이고 만일 지금 북한사역과 관련된 누군가가 주목을 받는다면 그 사역자 역시 북한 해커집단의 표적이 될 것이다. 상시적으로 북한사역을 이어가고 있는 선교단체에 대한 사이버 위협 역시 말할 나위 없을 것이다.

온라인 정보관리의 취약성

사이버보안과 관련한 미국의 베스트셀러 "사이버보안 어벤져스는 없다. (Cybersecurity and Cyberwar)"[2]를 쓴 두 저자는 책의 서론에서 저작 동기를 이렇게 설명한다. "모든 중요한 일들이 사이버를 통해 이루어지고 있는데도 사이버 보안에 대해 이해하지 못하고 '사이버 뭣들(All this cyber stuff)'이라고 설

1 "북한, 불법 가상화폐 탈취 최서 15억 달러... 거래소-ATM 등 공격.「VOA」, 2020년 9월 4일; https://www.voakorea.com/korea/korea-economy/norko-cyber-space-sanctions-evasion

2 피터 W. 싱어, 알란 A. 프리드만, 『사이버보안 어벤져스는 없다』(서울: 프리렉, 2016)

명하는 미 국방부의 고위 간부를 보고 책을 쓸 결심을 하게 됐다." 이 책에서 지적하는 바는 한 조직의 IT담당자가 무언가를 말하면 대부분 사람들이 그저 입을 다물고 고개만 끄덕이는 상황. 대화의 화제가 컴퓨터보안으로 넘어갈 때마다 너무나 확실하게 난처해하거나 무관심을 보이는, 그 결과, 조직 내의 사이버보안 구조가 기형적인 모습을 보이게 되는 상황이다. 저자들에 의하면 이시대의 사이버 보안은 조직의 담당자, 전문가만의 일이 아니며 구성원 모두가 내면화하고 주기적으로 업데이트 해야 할 사항이다. 이 지적은 오바마행정부 초기 〈포춘〉지 선정 미국 500대 기업 의 97%가 해킹을 당한 (나머지 3%는 해킹 사실을 숨기거나 인지하지 못한 것으로 추정되는) 시절의 이야기이지만 지금 한국의 단체들에게도 적용되는 이야기이다.

2013년 1월 오픈도어선교회 월간북한소식 권두칼럼을 준비하며 "이단의 북한선교"에 대해 조사한 적이 있다. 기존연구가 전무한 주제를 조사하느라 많은 어려움이 있었으나 의외로 쉬운 방법으로 여러 이단의 다양한 정보를 얻을 수 있었다. 방법은 단순했다. 일단 각 이단의 홈페이지와 이단교회들의 카페에 나온 자료들을 샅샅이 뒤져 최대한 자료를 확보하고 그것을 바탕으로 본 선교회 현장 사역자들과 커뮤니케이션하며 조사하는 것 이었다. 인터넷을 통해 자료를 수집하는 과정에서는 단체사람들이 자주 사용하는 언어와 선교현장의 언어를 키워드로 검색하여 새로운 특징을 발견하고 그 단어를 단서로 새로운 정보들을 추적할 수 있었다.

자료 조사 중 ㄹXX 교주 의ㄷXX 집단이 파송한 한선교사의 기도편지 파일들을 발견한 적이 있다. 일부 기도편지들은 아무런 장치 없이 홈페이지에 개제된 상태였으나 그중 한 기도편지는 한글파일로 작성되었으나 암호가 걸려있는 상태였다. 되는대로 이런저런 번호를 눌러보았는데 그 문서의 비밀번호는 다름 아닌 0000이었다. 그 편지를 통해 선교사의 가족사진과 ㄷXX집단이 단동에서 벌이고 있는 사역을 파악할 수 있었다. 당시 자료 조사 중 온라인에 공개된 ㄱX파 교주의 선교특강 에서 그 집단의 북한선교 정책에 대한 정보를 얻었고, 교주의 대표저작물이 중국의 어느 도시에서 우리말로 인쇄된다는 정보를 얻어 현장사역자에게 이를 알렸다. 그 과정에서 현장사역자도 그 이단의 문서사역을 감지하고 이단서적 인쇄를 막기 위해 노력하고 있는 것을 서로 확인한 경험이 있다.

2017년 2월 조중국경 선교사의 대규모 추방이 있은 직후 현장에서는 정통교단, 건전한 선교단체 선교사들이 빠진 틈을 타 이단이 활개 치기 시작했다는 소문이 돌았다. 당시 우연히 알게 된 한인들 중 기독교인으로 보이나 자신들은 무교라고 말하는 한인들이 있었다. 평소 같으면 '선교사님이신가보구나' 하고 넘어가겠지만 당시 이단이 활개 치기 시작한다는 소문이 있던 터라 그냥 넘어갈 수 없었다. 그들에 관한 정보들을 종합하여 구글링을 하였고 그들이 속한 교단, 출신 학교로부터 시작하여 후원교회에 이르는 일련의 정보를 얻을 수 있었다. 다행히도 그분들은 건전한 교단에 속한 선교사들이었다. 그 선교사님들은 자신의 신분을 감추기 위해 수많은 것을 포기하고 많은 노력을 하고 있지만 정작 그들의 신분은 이미 본인도 모르게 모두에게 노출되어있는 상황이다.

필자는 IT전문가도 아니고 정보-첩보활동을 위한 훈련을 받은 적 없는 일반인이다. 그럼에도 방에 앉아 위와 같은 많은 정보를 손쉽게 얻을 수 있었다. 전문 훈련을 받은 북한의 요원들은 필자보다 훨씬 많은 정보를 얻을 수 있을 것이며, 선교현지 정부의 공권력에 속하여 IT관련 권한을 갖춘 공안, 경찰들은 훨씬 더 많은 정보를 더욱 쉽게 얻을 수 있을 것이다.

선교현장 사이버보안의 기본원칙들

패스워드의 보호는 사이버 보안의 기본이다. 회원가입이 필요한 대부분의 사이트들이 패스워드를 복잡하게 설정하도록 강제하고 주기적으로 변경하도록 강요하는 것은 업체 차원에서 보안을 위한 필수적인 장치이다. 패스워드 관리를 위해 사용자 차원에서 추가적으로 신경 쓸 부분으로는 ①중요한 사이트간의 패스워드를 다르게 설정 ②공공장소 컴퓨터에서 개인계정으로 로그인 하지 않기 ③불필요한 홈페이지에 회원가입하지 않고 더 이

〈https 적용 웹페이지는 웹브라우저에서 자물쇠 표시(좌측 그림)로 확인이 가능하다. 반대로 미적용 사이트의 경우 '안전하지 않음' (우측 그림) 표시가 보이게 된다. 실제 네이버는 https를 적용한 안전한 사이트이지만 네이버를 가장한 사이트의 경우 '안전하지 않음' 표시를 볼 수 있다.〉

상 이용하지 않는 사이트 탈퇴하기[3] 등이 있다. 최근 강력한 보안을 갖춘 사이트를 중심으로 2단계 인증을 제공하는 추세인데 2단계 인증을 사용하면 훨씬 더 강력한 패스워드 보안을 유지할 수 있으므로 가능하면 2단계 인증을 사용하여야 한다. 또한 많은 사이트들이 회원가입을 하지 않고 구글계정, 네이버계정 등으로 로그인 할 수 있도록 서비스를 제공하고 있는데 이때는 구글, 네이버 등의 계정으로 로그인 하는 것이 더욱 안전하다. 이는 소규모 사이트에 비해 대형 포털의 유저, 비번 관리시스템이 더욱 강력하기 때문이다.

2018년 북한관련 단체들에 대한 해킹시도가 여럿 보도되었는데 대부분이 이메일을 통한 악성코드 유포의 시도였다. 가령 대북사업 관련 자료를 첨부한 것으로 가장하여 메일을 보내는 경우, 연구자와 전문가에게 취업제안을 가장한 메일을 보내어 클릭을 유도하는 경우 등이 있다. 최근에는 대북방송단체인 자유아시아방송에 "월간북한동향 2020년 11월호" 라는 제목의 전자우편을 보내 클릭을 유도하여 해킹을 시도한 사례도 포착이 되었다. 대부분의 경우 메일의 양식과 디자인, 보낸 사람의 주소에 이르기까지 수신자들이 의심하기 어려운 형태로 진화하고 있다.

인터넷 브라우저에는 엣지, 크롬, 파이어폭스 등이 있다. 인터넷 사용을 위해 브라우저들이 필수로 사용되므로 브라우저는 사이버 공격자의 표적이 되므로 사용자들은 항상 브라우저를 최신으로 업데이트 해야 한다. 같은 이유로 컴퓨터와 스마트폰의 모든 프로그램들은 늘 업데이트하여 항상 최신의 상태를 유지해야한다. 과거 많이 사용되던 인터넷 익스플로러는 더 이상 보안 패치 등 서비스가 제공되지 않으므로 사용하지 말아야한다.

개인의 프라이버시가 공개되는 가장 주요한 통로는 SNS이다. SNS를 통해 이용자의 출신지, 출신학교, 사회활동이 노출되며 사용자 본인의 의지와 상관없이 다른 사용자에 의해 태그되거나 사진이 노출되는 경우가 많다. 과거 북한선교 현장에서 큰 사건이 터졌을 때 그 사건을 파악하기 위해 며칠간 관련 키워드로 주요 포털사이트를 검색하며 모니터한 경험이 있다. 당시는 다음과 카카오스토리의 합병 초기라 카카오스토리의 내용들이 다음에서 검색이 되던 시절이다. 사건 직후 한 선교사가 카카오를 통해 공유한 사건과 관련된 매우 민감한 내용들(실제로는 정직하지 않은 내용이었음)이 공유되는 과정을 다음 포털검색을 통해 실시간으로 지켜본 기억이 있다. 또한 본인의 사회관계망이 노출된다는 것은 나와 관련된 정보를 제공할 수 있는 사람들이 노출된다는 것을 의미한다. 본인의 사역을 노출시키지 않기 원한다면 SNS의 탈퇴 혹은 비활성화는 필수이다.

가정-사무실의 보안환경과 여행지의 보안환경에는 매우 큰 차이가 있다. 가정-사무실과 달리 여행지에서 접속하는 네트워크는 대부분 우리가 전적으로 신뢰할 수 없는 네트워크이며 여행지에서는 기기의 도난 위험도 증가한다. 민감한 현장의 경우 스마트폰과 노트북에 대한 검열이 이루어지는 경우도 있다. 그러므로 여행할 때 챙겨가는 전자기기에 필요 없는 데이터가 무엇인지 파악하고, 불필요한 정보는 삭제해야한다. 출장용 기기를 따로 구비하는 것도 하나의 방법이다. 전자기기의 잠금 설정은 필수이며 스마트폰의 도난 분실 시 대부분의 스마트폰에서 제공하는 원격 데이터 접근차단 삭제기능을 실행할 수 있어야 한다. 여행 중 인터넷 접속을 위해 와이파이를 많이 사용하는데 공공와이파이는 기본적으로 근처에 있는 누구나가 통신을 가로채거나 모니터링 할 수 있고 출처를 알 수 없는 와이파이는 해킹을 위한 도구일 확률이 높다. 그러므로 공공와이파이를 사용할 경우 방문하는 웹사이트가 암호화되고 있는지 확인(URL에 https://를 사용하고 잠금장치 이미지가 있음)하거나 VPN을 사용하여야 하는데, 이러한 기술을 사용하기 어려운 경우 핸드폰 요금이 들더라도 모바일 데이터를 사용하는 것이 안전하다.

맞춤형 사이버 보안

중국에서 활동하거나 활동한 경험이 있는 선교사들과 이야기하며 듣는 보안관련 이야기들 중 가장 답답한 말이 "어차피 중국 공안은 누가 선교사고 어디서 무슨 일 하는지 100%다 안다."는 말이다. 이 말은 반은 맞고 반은 틀린 말이다. 이 글의 앞부분에서 말했듯 현지의 공권력은 선교사의 사역을 간파할 충분한 역량을 갖추고 있다는 점에서 이 말에는 일리가 있다. 그러나 현지의 공안이 그 많은 외국인의 일거수일투족을 감시할 수 없다는 점에서는 이 말은 틀린 말이다. 개인에 대한 감시와 뒷조사에는 많은 비용과 인력이 소모된다. 현지 공안들은 크게 의심 살 일 없는 외국인들에게 그렇게 많은 에너지를 쓸 만

3 한국인터넷진흥원의 정보클린센터(http://www.eprivacy.go.kr/) 에서는 개인의 회원가입 정보검색 서비스를 제공한다.

큼 한가한 사람들이 아니다. 물론 누가 봐도 선교사임에 틀림없는 사람이 여기저기 다니며 드러내놓고 선교사역을 한다면 공안이 아니라 동네사람들도 그 선교사의 사역을 다 알 것이다. 그러나 만일 어떤 선교사가 현장에서 적절한 신분을 갖고 본인이 드러나는 상황을 최소화 하고 보안에 신경 쓰며 사역한다면 그 선교사가 노출될 확률은 보안개념 없이 사역하는 선교사에 비해 현저히 줄어든다. 물론, 북한선교 관계자들과 현장사역자들이 자신과 사역의 노출 확률을 0%로 줄이는 것은 불가능한 일이므로 늘 겸손한 자세를 유지하며 주님만을 의지하여야 할 것이다.

한국의 북한선교계에 보안과 관련된 이야기들 중 상당수는 보안에 신경을 많이 쓰지 못해 어려움을 겪은 분들의 이야기들이다. 자신이 보안에 노력과 재정을 쏟지 않으니 다른 이들도 자기와 같을 것으로 생각하는 사람들도 매우 많다. 보안문제에 있어 잘 준비되고 철저하게 사역하는 선교사들이 이들과 같이 도매금으로 매도되지 않기를 바란다. 지금도 현장에는 수많은 사역자들이 지혜롭게 사역을 이어가고 있으며 그들의 보안 노하우는 공개되지 않는다.

북한선교 관련단체와 현장사역자 대부분은 현장에서 보안관련 공권력의 도움을 받기 어려우며 예산에도 많은 제한이 있다. 그러나 시중에는 인터넷, 스마트폰 보안과 관련하여 수많은 도서들이 출판되어있으며 최근에는 유튜브를 통해서도 많은 정보들이 제공되고 있다. 하다못해 유튜브에 있는 해외 탐정들의 노하우들과 국내 사설 흥신소의 무용담 속에서도 우리는 보안에 대한 많은 통찰을 얻을 수 있다. 이 글을 포함한 월간 북한 소식의 3월호 글들이 북한선교계와 현장 사역자들이 사이버 보안 관련 노하우를 쌓는데 의미 있는 도움이 되기를 바란다.

북한의 사이버 위협과 예방법

문 동 희 (데일리 NK)

김정은은 집권 초기인 2013년 간부들에게 "사이버전은 핵, 미사일과 함께 인민군대의 무자비한 타격 능력을 담보하는 만능의 보검"이라고 강조한 바 있다. 북한의 해킹 수준은 세계 최고로 평가받는 미국, 러시아, 중국 등과 어깨를 나란히 할 정도로 높다. 기술의 발전으로 많은 사람이 언제 어디서나 네트워크에 접속할 수 있는 기기를 이용하고 있지만, 많은 사람이 해킹, 보안 문제에 대해서 둔감한 편이다. 더 큰 문제는 이미 해커의 공격에 노출돼 정보가 빠져나가고 있지만, 해킹 공격을 받았다는 사실 조차 모르는 사람도 상당하다는 것이다. 시간과 공간에 구애받지 않고 은밀하게 우리 생활을 파고드는 북한 사이버 공격에 경각심을 가지고 대처해야 한다.

북한 해킹 조직

북한 참모부 산하 기술정찰국은 북한 대표적인 해킹조직의 활동을 배후에서 지휘하는 조직이다. 기술정찰국은 3국으로 통칭하며 사이버 지도국, 121국 등으로도 불린다.

미국 육군이 지난해 발간한 '북한 전술(North Korean Tactics)' 보고서에 따르면 121국은 총 4개의 산하 조직이 있다. 121국은 사회적 혼란이 주요 목적인 '라자루스(The Lazarus Group)', 적으로부터 정보를 수집하는 '안다리엘(The Andarial Group)', 금융 사이버 범죄를 지휘하고 있는 '블루노로프(The Bluenoroff Group)', 그리고 북한 내에는 '전자전 교란연대(Electronic Warfare Jamming Regiment)'으로 구성됐다.

라자루스는 지난 2016년 방글라데시 중앙은행을 공격해 8,100만 달러(당시 한화 약 906억 원)를 훔친 배후로 지목됐다. 라자루스는 2014년 김정은 암살을 소재로 한 영화 '인터뷰'를 제작한 미국 영화사 소니픽처스를 해킹했다. 그리고 2017년 150여개 국 컴퓨터 30만대에 피해를 준 '워너크라이' 랜섬웨어 사건과도 밀접한 관련이 있다.

안다리엘과 블루노로프 금융 전산망 등을 공격해 불법으로 돈을 탈취하고 있다. 미국

〈북한 해커 박진혁에 대한 미 FBI의 공개 수배 전단. 박진혁 씨는 북한 해커 조직 라자루스(Lazarus) 그룹에 속해 활동하는 것으로 알려졌다.〉

재무부가 지난해 발표한 '2020테러리스트 및 기타 불법 자금 조달 대응 국가 전략' 보고서에 따르면 라자루스를 비롯한 북한의 3개 해킹조직은 2017~2018년 아시아의 5개 거래소에서 암호화폐 5억 7,100만 달러(약 7,000억 원)를 탈취했다.

라자루스 등이 해외의 정부, 금융기관을 노린다면 북한의 또 다른 해킹 조직 금성121과 김수키(Kimsuky)는 국내가 주 활동 무대이다. 금성121과 김수키는 북한과 관련된 활동 및 연구를 하는 국내 거주 탈북민, 전문가, 정치인, 언론인 등을 주공격 대상으로 삼고 있다.

북한의 해커는 약 7,000여 명으로 알려져 있으며 벨라루스, 중국, 인도, 말레이시아, 러시아 등지에서 활동하는 것으로 알려졌다.

북한 국내 사이버 공격 사례와 예방법

이 글에서는 북한이 국내에서 실시하는 사이버 공격 중 개인을 대상으로 한 사례들을 이야기하려 한다.

〈백신 업체 소포스(Sophos)의 피싱 템플릿 예시. 해당 메시지에 따라 클릭하면 계정 로그인을 요구하는데 실제로는 가짜 로그인 창을 띄워 정보를 탈취한다〉

우선 가장 많은 사례는 포털사이트나 관련 사이트의 로그인 창을 띄워 로그인을 다시 하라고 유도하는 방식이다. 해외 로그인 시도, 세션 만료, IP 변경, 오래된 비밀번호 등 다양한 이유를 설명한 뒤 로그인을 유도하기도 한다.

포털 사이트 고객센터를 위장해 해커가 만들어 놓은 사이트로 유도해 로그인하는 방법은 고전적인 방식이나 여전히 시도되고 있다. 고전적인 방식이지만 이에 속아 넘어가는 사람이 아직도 많기 때문이다.

〈최근 연말정산 시즌에 맞춰 특정 재해구호협회 단체에서 발송한 것처럼 위장한 해킹 이메일. (이스트시큐리티/데일리NK 보도사진 재인용)〉

이를 예방하기 위해서는 이메일을 통해 로그인을 유도하거나 고객센터로 안내하는 메일은 무시하고 비밀번호를 직접 계정 설정에 들어가 변경하는 것이 좋다. 계정과 관련한 다른 모든 일도 링크를 통해서가 아닌 직접 계정 설정에 들어가서 하면 개인정보 유출을 막을 수 있다.

네이버의 경우 실제 고객센터에서 보낸 이메일은 녹색 'N'자 아이콘이 있다는 점도 참고하면 좋다.

다음으로는 지인을 사칭한 사례들이다. 지인 이름으로 발송된 이메일에 대해서 많은 사람은 크게 경계심을 가지지 않는다. 해커는 이를 노리고 발신자를 조작한 메일을 공격 대상자에게 보낸다. 해커들에게 이메일 주소나 발신자명을 조작하는 일은 매우 간단하고 쉬운 일이다.

사회공학기법(Social Engineering)을 활용해 지인, 지원 등을 미끼로 공격 대상자를 현혹하는 피싱(Phishing) 이메일을 발송하는 것이다, 사회공학기법을 이용한 해킹은 시스템이 아닌 사람의 취약점을 공략해 정보를 탈취하는 방식이다.

같은 기관의 동료가 보낸 보고서, 피드백 요청, 외부 업체의 견적서와 계약서, 후원 신청서와 기부금 영수증 등이 모두 해커가 이용할 수 있는 수단이다. 평소 지인이나 외부기관과 주고받는 사적 혹은 업무 문서가 피싱에 활용되는 경우가 있다는 이야기이다. 실제, 금성121은 지난 2019년 실제 사용되는 '제17기 북한선교학교 신청서'라는 문서를 활용해 특정 선교 단체를 공격한 바 있다. 지인을 사칭한 피싱 공격을 예방하기 위해서는 해당 메일이 본인이 받을 만한 내용인지 의심하고 발신자에게 이메일 발송 여부를 확인하는 편이 좋다.

북한 해커들은 지인과 주고받는 문서가 아니더라도 공격 대상자의 호기심을 자극할만한 자료들을 활용하기도 한다. 기자들에게는 통일부에서 발송한 보도자료, 각종 현안 분석 자료, 북한 관련 NGO에게는 탈북민의 기구한 사연, 기부 정보, 북한 내부 소식 등을 미끼로 사용하기도 한다. 선교 관련 기관에는 북·중 국경 상황, 북한 내부 선교 정보, 중국 내 탈북민 현황, 탈북민의 한국행 도움 요청 등을 활용한 방법이 사용될 가능성이 높다.

북한 해커들은 지인 사칭뿐만 아니라 사

회적인 관심을 받는 이슈를 활용해 해킹에 활용하는 경우도 있다. 남북정상회담, 북미 정상회담 시기에는 국책연구기관으로 위장해 관련 분석 자료를 보내기도 하며 연초에는 북한 신년사를 활용한다. 북한 해커들은 미국 대통령 선거 기간에는 대선을 분석한 자료를 이용한 공격을 시도하기도 했다.

세 번째로 파일을 이용한 사이버 공격이다. 보통 해커들은 이메일에 악성 파일 첨부해 보낸다. 악성 파일의 경우 크게 설치 파일과 문서 파일로 나눠진다. 첨부파일을 다운로드 받지않는 것이 가장 좋은 방법이지만 실수로 받았더라도 실행을 시키지 않아야 한다. 문서의 경우 한글(hwp), 워드(doc), 엑셀(xls)의 매크로 기능과 프로그램 취약점을 이용한다. 문서를 실행하면 매크로 실행 버튼 클릭을 유도한 뒤 버튼을 누르면 정상화면을 보여준다. 이때 보이지 않는 백그라운드에서는 해커가 미리 설정해둔 서버와 통신해 악성 프로그램을 다운로드하고 설치하는 과정이 이뤄진다. 사용자에게 정상화면을 보여주는 이유는 해킹 여부를 숨기기 위한 해커의 전략이다. 이 때문에 실수로 악성 문서를 열었더라도 매크로 실행 버튼을 누르지 않으면 감염되지 않는 경우가 있다. 그렇지만 해커가 문서 프로그램의 취약점을 이용해 공격한 경우에는 매크로와 관계없이 실행만으로 악성코드에 감염된다. 의심스러운 파일은 열어보지 않도록 주의해야 한다. 문서 프로그램의 취약점은 제조사에서 보안 패치를 이미 완료했다. 이에 문서프로그램을 항상 최신 버전으로 유지하는 게 악성코드를 실행을 막는 방법 중 하나이다.

마지막으로 스마트폰을 이용한 공격이다. 최근 북한은 PC를 넘어 스마트폰까지 공격 대상으로 삼고 있다. 스마트폰은 특성상 24시간 사용자와 함께한다는 점에서 감염될 경우 일반 PC보다 더 큰 피해를 받을 수 있다. 해커들은 사용자들이 PC보다 스마트폰 보안 의식이 취약하다는 점을 노리고 있다.

스마트폰이 악성 앱이 설치되면 녹음기능, 위치추적을 통해 음성통화뿐만 아니라 일상적인 대화까지도 녹음될 가능성이 크며 실시간 이동 경로가 해커에게 전달될 수 있다. 스마트폰이 실시간 위치추적이 가능한 도청기가 될 수 있다. 여기에 스마트폰 내부의 연락처, 사진, 문자 메시지 등의 은밀한 정보가 해커에게 유출돼 2차 피해가 발생할 우려도 있다.

지난 2019년에는 '북한이탈주민 모금 운동'이라는 웹사이트를 만들고 가짜 모바일 메신저 앱인 'X helpers' 설치를 유도했다. 당시 해커는 공격대상자들에게 이메일 발송, 페이스북, 유튜브를 통해서도 가짜 웹사이트 방문과 악성 앱 설치 유도하는 등 집요한 모습도 보였다.

공식 마켓에서 다운받은 검증된 앱 이외에는 가급적 설치하지 않는 것이 해킹 피해를 예방하는 방법이며 지인이 보낸 URL이

〈탈북민에게 카카오톡 메신저로 악성 앱을 전달하는 사례. (이스트시큐리티)〉

나 파일이더라도 주의 깊게 확인해야 한다. 그리고 가급적 전화 통화로 사실 여부를 확인하는 습관이 중요하다.

또한, 알 수 없는 사람에게서 오는 카카오톡 메시지의 경우 상당히 조심해야 한다. 외국의 사업가, 북한에 관심이 많은 선교사, 탈북민으로 위장해 공격대상자에게 접근하는 경우가 많다. 이런 해커들은 처음부터 공격을 시도하지 않고 오랜 시간에 걸쳐 카카오톡 등으로 대화를 하면서 신뢰도를 높이는 방법을 사용한다. 또한, 처음에는 정상파일을 주고받아 상대방을 안심시키다가 일정 시간이 흐른 뒤에 악성 파일을 보낸다. 특히, 보안 메신저를 이용해야 한다면서 접근하는 사람을 조심해야 한다.

북한 해커는 이 앱과 별도로 '쓰리마(Threema)', '위커(Wickr)' 등 실제 존재하는 보안 메신저도 유포하기도 했다. 조작된 안드로이드 앱 패키징 파일(APK)을 설치하도록 유도하는 것이다. 해당 메신저들은 해커에 의해 조작된 악성 앱으로 설치 시 사용자 정보가 모두 탈취된다.

전 세계 스마트폰 점유율이 70%가 넘고 외부에서 받은 앱 설치가 자유로운 안드로이드 기반 휴대전화가 북한 해커들의 주요 표적이다, 아이폰은 상대적으로 보안에 유리한 측면이 있다. 이와 비슷한 맥락으로 북한 해커들은 윈도 기반 PC를 중점적으로 노리는 만큼 Mac OS를 이용하는 것도 해킹 예방에 도움이 된다.

마치며

개인정보 보호는 누구에게나 중요한 문제이다. 그러나 북한과 밀접한 관련이 있는 사람의 개인정보 노출될 경우 매우 치명적인 결과를 낳을 수 있다. 중국이나 북한에 있는 정보원, 협력자의 신분이 노출돼 신변에 큰 문제가 발생하는 일의 출발점이 본인이 될 수 있다. 북한이 사용하는 사이버 위협이 대부분 사람의 심리를 노리고 있어 개인이 보안 문제에 경각심을 가지면 해킹을 충분히 방지할 수 있다. 또한, 개인뿐만 아니라 단체에서도 정기적으로 보안 교육을 해 북한의 사이버 위협으로부터 기관과 구성원들의 안전을 지키는 노력을 할 필요가 있다.

선교 보안의 기본 - IT 보안을 중심으로

다 니 엘 (기술과학전문인선교회(FMnC) 사역자)

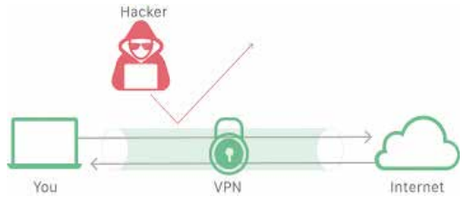
은폐와 암호화

선교에서 보안은 매우 중요하다. 선교 금지 국가에서 중요한 정보가 노출되면 모든 사역이 한순간에 멈출 수 있기 때문이다. 그렇지만 정보 유출을 막는 것이 생각만큼 녹록치 않다. 상당수의 선교지가 선교 사역이 불법일 뿐 아니라 정부에 의해 강력한 정보 통제나 감시가 이루어지고 있기 때문이다. 선교지에서 중요한 대화를 하는 상황을 생각해보자. 작은 목소리로 대화를 하더라도 도청기가 설치되어 있다면 결국 대화 내용은 도청되고 보안은 유지될 수 없다. 온라인도 마찬가지이다. 기술의 발달로 스마트폰에서 또는 인터넷상에서 키보드로 입력하여 인터넷 상에서 전송하는 모든 정보는 다 도청, 감청이 될 수 있다.

그러면 이러한 도청, 감청을 회피하는 방법은 무엇일까? 가장 기본적인 방법으로는 "은폐"가 있다. 정치인들이나 범죄자들이 대포폰을 쓰는 것은 자신의 신분을 노출시키지 않기 위해서이다. 선교현장에서도 비슷한 원리가 적용된다. 즉 신분 노출을 피하고자 한다면 해킹을 시도하려는 공격자로부터 표적이 어디인지 모르도록 조치해야 한다는 것이다. 이는 개구리가 보호색을 사용하고 군인들이 감청색 옷으로 은폐하는 것과 비슷한 이치이다.

다음으로 중요한 방법은 암호화이다. 가장 간단한 암호화의 예를 들자면 일상생활에서 대화를 할 때 중요한 핵심 키워드를 모두 치환해서 다른 단어로 대화하는 것이다. 북한의 간첩이 한국에 오면 성경책으로 지령을 내린다는 이야기를 들은 적이 있다. 대부분의 단어가 성경책에 들어있기 때문이다. 그래서 통신상에서는 직접적인 단어를 표현하지 않고 몇 장 몇 절 등으로 치환해서 통신하는 식이다.

치환을 이용한 암호화로 인한 해프닝도 있었다. 96년 간첩 이광수 씨가 붙잡혔을 때 광어가 먹고 싶다고 발언했는데, 기자들이 도대체 저건 어떤 암호문일까 하고 궁금해 했고 이에 대한 여러 가지 추측이 나돌기도 했다가 나중에서야 별 의미 없는 발언이었음이 드러나기도 했다. 여하튼 다른 단어로 특정 의미를 전달하는 것은 치환을 통한 암호화라고 할 수 있다. 이러한 암호화 기법은 평소 문자나 통화에서는 사용할 수 있지만 모든 영역에 적용할 수는 없다. 특히 디지털 시대 온라인상의 자료 왕래가 빈번한 상황에서 단순한 치환을 통한 암호화는 한계가 분명하다.



〈가상사설망(VPN)을 표현한 도식 (Cloudflare 홈페이지 캡처)〉

그렇다면 인터넷이나 스마트폰에서 암호화를 하는 가장 쉬운 방법은 무엇일까? 첫 번째로 소개할 내용은 가상사설망(VPN)이다. VPN은 가상으로 원격지를 사설망(로컬망)에서 접속하는 것처럼 터널을 맺어서 암호화 주는 기술이다. 사용자의 정보를 암호화하여 보안을 향상시킨다.

이미 시중에는 다양한 VPN 서비스가 제공되고 있다. 스마트폰에서도 구글 플레이나 앱스토어 또는 크롬 웹스토어에서 VPN을 검색하면 다양한 무료 VPN 암호화 앱을 설치할 수 있다. 물론 모든 VPN이 다 신뢰할 수 있는 서비스를 제공하는 것은 아니기에 확인이 필요하다.

그 외에도 텔레그램 등의 보안성 높은 메신저나 Protonmail 과 같이 보안성이 높은 메일을 사용하는 것도 효과적이다. 다만 선교현장에서는 사용하기 어려운 방법인데, 이러한 메신저나 서비스에 접속하는 것 자체가 의심을 살 수 있는 일이기 때문이다. 중국의 대대적인 VPN 단속 등은 이미 잘 알려진 사실이다.

또한 웹브라우저에서는 무조건 홈페이지 주소 앞부분이 https 로 된 곳에서만 정보를 입력하는 습관을 가져야 한다. https는 기존 웹사이트의 http에서 보안이 강화된 버전으로서 서버와의 통신 데이터를 암호화한다. 일일이 https를 확인하고 접속하기 어렵다면 구글에서 "HTTPS everywhere" 를 검색해서 크롬(Chrome) 웹브라우저에 설치하면 무조건 https 로만 접속되도록 강제할 수가 있다. 이렇게 설정하고 크롬으로만 인터넷을 사용한다면 좀 더 안전할 수 있다.

데이터 관리의 중요성

암호화나 은폐는 보안의 기본이라고 할 수 있지만 근본적으로는 민감한 정보들이 유출되는 것을 물리적으로 차단하는 것이 좋다. 선교 현장에서는 노트북이나 PC에는 절대

중요한 정보는 저장하지 않아야 한다. 또 노트북이나 PC의 브라우저에 비밀번호 자동 저장 기능이나 중요한 정보가 있는 페이지는 북마크를 하지 않아야 한다. 최근 일부 보안 메일 사이트의 경우 압수를 당해서 로그인을 하라고 강요를 당할 경우 비밀번호를 몇 회 이상 틀리면 정보가 초기화되는 기능을 지원하기도 함으로 이를 지혜롭게 활용하는 방안도 제안해본다.

클라우드를 선교에 활용하려고 한다면 단체나 교회의 자체 서버보다는 시중에 보급된 주요 기업의 클라우드가 덜 위험할 수 있다. 개개의 서버는 직접적인 해킹의 표적이 될 수 있지만 대형 클라우드 업체는 상대적으로 위험이 적기 때문이다. 또한 현지 선교사가 교회나 선교 단체의 서버를 자주 접속할 경우 아이피 추적을 통해 선교사 신원이 드러날 위험이 있으므로 이에 대한 주의가 요구된다.

전문가의 도움을 받는 것도 좋은 방안이다. 닷네임코리아 (www.dotname.co.kr)에서는 선교 관련 클라우드 활용 및 IT보안 향상을 위한 다양한 툴과 솔루션을 제공하고 있다. 이런 전문 업체들을 활용하거나 전문가의 조언을 통해 전반적인 선교 단체 IT 시스템의 보안성을 높이는 것도 도움이 될 것이다.

사회공학적 해킹이란

보안은 결국 사람이 지키는 것이다. 앞서 언급한 일부 기술적인 장치도 도움이 되겠지만 근본적으로는 선교사와 단체가 스스로 보안을 지키는 것이 중요하다. 특히 최근 사이버 공격은 사회공학적인 수법을 많이 이용한다. 정보 보안에서의 사회공학은 사용자를 속이거나 공격자의 신분을 감춘 상태로 사람들을 교묘히 조종하는 것을 의미한다. 즉 사회공학적 해킹은 시스템이 아닌 사람의 취약점을 공략하여 원하는 정보를 얻는 공격 기법을 통칭한다. 전화사기, 이메일 피싱, 우편물 등을 통한 개인 정보 도난 등 특별한 기술 없이도 손쉽게 기본 정보를 얻어내는 비 기술적인 침입 방법이라고도 한다. 사회공학적 기법은 일반적인 해킹보다 더욱 심각한 문제이다. 원래 사람이란 예측 불가능한데다 조작이나 설득에 걸려들기 쉬운 점을 악용하기 때문이다.

사회공학적 해킹 기법으로는 여러가지가 있다. 물리적으로는 직접 접근 방식이 있는데 조직에서 높은 위치에 있는 사람으로 가장하거나 긴급한 상황에서 도움이 필요한 것처럼 행동하는 것 등이다. 예를 들면, 어떤 일을 처리하지 못하면 자신이 무척 난처해지며 정상적인 절차를 밟기가 곤란하다고 호소하는 것이다. 또 가장된 인간관계 이용하기도 한다. 즉 조직 내의 개인 정보를 획득하여, 어떤 사람의 친구로 가장해 상대로 하여금 자신을 믿도록 한 뒤 정보를 획득하는 것이다. 그 외에 앞서 언급했던 도청도

〈가장된 인간관계를 이용한 사회공학적 해킹 메시지 예시〉

사회공학적 해킹의 일종으로 볼 수 있다.

온라인 영역을 생각해보면 인터넷 구글 등의 다양한 검색엔진 크롤링(crawling)도 일종의 해킹시도라고 할 수 있다. 크롤링은 인터넷에 존재하는 다양한 검색 엔진을 이용하여 인터넷에 존재하는 공격 대상과 관련된 개인 정보 및 사회 활동과 관련된 다양한 정보를 수집하는 방식이다. 이름, 소속단체, 직책, 주민번호, 주소, 전화번호, 이메일 등을 얻을 수 있다. 실제로 이 글을 읽으시는 독자나 독자의 지인에 대해 검색 사이트에서 키워드를 입력해보면 생각보다 많은 정보를 확인할 수 있을 것이다.

피싱(Phsing)은 잘 알려진 사회공학적 기법이다. 피싱은 개인정보 (Private data)와 낚시 (Fishing)의 합성어로 사람을 속이는데 초점을 맞춘 해킹 수법이다. 예를 들어 중요 문서가 첨부된 것처럼, 또는 아는 사람이 보낸 것처럼 가장된 이메일을 보내서 받는 이가 열어볼 수밖에 없도록 한 뒤 파일을 열면 컴퓨터를 감염시키거나, 또는 갑자기 네이버나 지메일 같은 사이트인 양 비번을 물어보는 창을 띄워서 로그인을 유도하여 아이디 비번을 탈취하는 것이다.

피싱에서 발전된 해킹 수법으로 파밍(Pharming)이 있다. 파밍은 피싱(Phishing)과 조작(Farming)의 합성어로, 악성프로그램에 감염된 PC를 조작하여 정상 사이트에 접속하더라도 가짜 사이트로 접속을 유도하여 정보를 빼돌리고 피해를 입히는 것을 말한다. 예를 들어 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나, DNS(도메인네임시스템)이름을 속여 사용자가 진짜 사이트로 오인하도록 유도하여 개인 정보를 훔치는 것이다. 즉 사용자는 내가 정상적인 잘 알려진 포탈, 메일, 은행 사이트를 접속한다고 생각하지만 사실은 유사하게 만들어진 가짜에 자기 정보를 입력하게 만드는 것이다.

사회 공학 기법의 공격 흐름과 각각의 대응

사회 공학 기법을 사용하는 공격자는 공

격 대상이 되는 특정 인물을 선정한 후 다음과 같은 흐름으로 사회 공학 기법의 공격을 진행하게 된다. 공격의 흐름에 대한 이해는 관련 피해 예방에 기초가 된다.

① 정보 수집

공격자는 먼저 공격 대상 관련 가족 관계, 직장 생활 그리고 사회 모임 등의 개인적이거나 사회적인 활동 등과 관련된 다양한 정보들의 수집을 시도하게 된다. 공격자는 이 단계에서 수집한 다양한 정보들을 다음 단계인 관계 형성을 위해서 사용하게 된다.

정보 수집 단계에서의 대응 전략은 공격자가 정보들을 수집하는 것을 사전에 어렵도록 하는 것이다. 특히 개인 신상 정보 관리가 중요하다. 단체가 관리하는 신상 정보는 물론이고 세금, 일반 요금 고지서, 신용카드 영수증 및 송금 전표 등 신상 관련 정보를 유추할 수 있는 문서들은 함부로 휴지통에 버리지 말고 파쇄 하도록 한다. 또한 온라인상에 신상을 기입할 경우 불필요하게 자세한 정보를 기입하지 않고, 단체 홈페이지나 블로그 등과 같이 외부에 알려져 있는 공간에 신상을 노출하지 않아야 한다.

② 관계 형성

공격자는 공격 대상과 관련된 다양한 정보들을 충분히 수집하였다고 판단할 경우, 공격자는 이제 공격 대상과 직접적인 관계를 형

성하기 위해 2 단계인 관계 형성 단계로 발전시킨다. 물론 여기서 직접적인 관계는 사실 진짜 관계가 아닌 공격자가 자신을 '가장' 하여 속이는 것이다. 즉 공격 대상에게 자신의 본 모습을 숨기고 다른 누군가로 위장하여 접근하게 된다. 이렇게 다른 누군가로 가장하여 공격 대상에게 접근하는 것은 공격 대상이 가질 수 있는 경계심을 없애고 신뢰할 수 있는 사람이라는 신뢰감을 형성하기 위한 것이다. 이 신뢰감을 바탕으로 공격자는 자신이 가진 특수한 목적을 달성하기 위한 사항을 다음 단계인 공격(Exploitation)에서 요청하게 된다.

③ 공격, 침투

세 번째 단계인 공격 및 침투는 공격자가 수집한 다양한 정보들을 바탕으로 공격 대상과 충분한 신뢰감을 형성하였다고 판단할 경우에 진행하게 된다. 이 세 번째 단계로 넘어가기 위해서는 공격자 자신을 공격 대상이 더 이상 의심하지 않는다는 판단이 중요하게 작용하게 된다. 이러한 신뢰 관계가 충분히 형성이 되면 공격자는 자신의 특수한 목적을 이룰 수 있는 사항을 공격이라는 단계에서 공격 대상에게 특정한 행위를 요청하게 된다.

공격 단계에서의 대응 전략은 공격자가 자신의 특수한 목적을 수행하기 위한 사항을 요청하더라도 공격 대상이 이를 거부함으로써 실행되지 않도록 방해하는 것이 주된 목적이다. 먼저 공격자로 의심되는 사람의 신분을 그 사람이 밝힌 소속 기관 및 기업 등에 연락하여 정확한 신분을 재확인하도록 한다. 그리고 요청한 사항이 실제로 해당 기관 및 기업에서 진행하고 있는 사항인지를 확인하도록 한다. 기술적으로는 방화벽과 UTM을 설치해서 해킹이 불가하도록 방어를 하도록 한다.

④ 실행, 탈취

실행, 탈취 단계에서 공격 대상은 공격자가 요청한 사항에 대해 직접적인 실행으로 옮김으로써 이로 인해 실질적인 피해가 발생하게 된다. 그리고 공격자는 요청 사항으로 인해 확보한 유형의 또는 무형의 신분을 이용하여 실질적인 목적을 수행할 수 있게 된다.

이 단계에서는 사고 예방 차원에서의 접근이 아니라 사고 대응 차원에서 접근하게 된다. 즉 유출된 정보를 공격자가 특수한 목적으로 활용하지 못하도록 하여 피해를 최소화는 것이다.

구체적인 IT 보안 실천사항

최근 가장 자주 접하게 되는 해킹 방식은 피싱 메일/메시지이다. 경우 열어볼 수밖에 없는 제목의 메일을 보내 첨부파일을 열게 되면 자연스럽게 피싱(네이버, 다음 등) 페이지가 띄워져서 메일 계정 비번을 탈취하거나, 또는 메일의 첨부파일을 열었을 때 백도어나 해킹 프로그램이 설치되어 있어 정보가 탈취당하는 사례이다. 특히 첨부파일이 정상적인 워드나 한글 파일 인 것처럼 위장되어 있지만 해킹프로그램이거나 악성 코드가 작동하게 되는 것이 일반적이다.

그렇기에 메일 발송자가 누군지 모르는 곳에서 보낸 첨부파일은 절대 열지 않도록 한다 (한글HWP, 엑셀, 워드, PDF 등). 크롬 브라우저 확장프로그램인 Malwarebytes Browser Guard 등을 설치하면 피싱을 탐지할 수 있다. 그 외에도 선교 단체 인터넷 회선에 UTM 방화벽을 구비하여 외부에서 단체로 침투를 하지 못하도록 방어하는 것도 필요하다.

스마트폰의 경우에도 모르는 사람이 보내는 메일이나 메시지(카톡 등 메신저 포함)는 열지 않는다. 해커가 보낸 것이라면 개봉할 때 아이피가 노출되어 해킹의 표적이 될 수 있기 때문이다. 또한 개인정보(핸드폰, 이메

일)가 인터넷에 노출되지 않도록 주의하고 노출된 메일이나 핸드폰 번호로는 중요 정보를 주고받는 목적으로 사용하지 않아야 한다. 또한 아는 사람으로 가장하여 톡이 올 수 있으니 첨부파일은 열지 않고, 열어야 한다면 Security360 등 스마트폰 용 백신을 설치하고 백신에서 제공하는 Sand Box 기능을 사용해서 파일을 열어야 감염이 되지 않는다.

선교 관련 자료 관리도 주의해야 한다. 주요 인명을 주소록을 만들어 파일로 관리하는 것은 매우 위험할 수 있으므로 파일로 만들어야 하는 경우 모든 이름 등은 모두 닉네임 등으로 치환하여 관리해야 한다. 또한 가급적이면 파일보다는 출력된 형태로 보관 후 파일은 삭제하고 복사본으로 관리하는 것이 좋다. 휴대폰의 주소록도 전화번호나 이름을 적절하게 바꿔서 사용해야 한다.

홈페이지나 페이스북 등 SNS 등에 선교사에 대한 기도제목이나 선교와 연관 있는 분의 사진 등을 기재하는 일은 당연히 삼가야 한다. SNS는 아주 쉽게 정보를 수집당하는 채널이기 때문이다. 서버 DB나 웹상에 올리는 정보는 모두 해킹당할 수 있다는 생각을 하고 절대로 중요한 핵심적인 정보는 공유하거나 업로드 하지 않아야 한다. 부득이하게 기도제목을 외부에 공유하여야 하는 경우에는 이메일로, 그리고 이미지로 모두 변환하여 텍스트로 검색되지 않도록 하는 것이 그나마 안전하다.

사회공학적 공격의 장기적 예방을 위해서는 적절한 시스템 구축과 교육이 필수적이다. 정기적인 교육 및 모의훈련을 실시하여 철저한 보안 의식 수립이 가장 핵심적 요소이다. 이러한 교육을 위한 가이드라인을 마련, 배포도 병행되어야 할 것이다. 또한 시스템 차원의 대비책을 통해 사용자의 실수를 최소화하는 체계를 구축해야 한다. 사용자의 부주의를 예방할 수 있는 업무 프로세스 및 기술을 적용하고, 주요 정보에 대한 모니터링 시스템 구축해 적법한 보안단계를 거치지 않고는 외부 유출이 불가능하도록 시스템을 구축한다.

마지막으로 새로운 유형의 사회공학적 해킹에 대해 연구하고 신속하게 대처할 수 있는 본부 차원의 체계를 구축해야 한다. 즉 계속해서 배우고 발전해야 한다. 정보기기의 종류와 활용 범위 증가, 새로운 IT 서비스의 증가로 인해 예상하지 못했던 새로운 사회공학적 공격 방식이 나타날 수 있기 때문이다.

라디오, 연변 냉면, 그리고 안전 가옥 (2)

편집부

안전 가옥에서의 삶이란

언뜻 그의 이야기를 들어보면 안전가옥이라는 곳은 아주 고요하고 평화로운 곳 같이 들리기도 한다. 사람들과 함께 먹고 마시며 기도와 하나님의 말씀을 읽는데 전념하는 그런 거룩한 곳이라 여겨지기도 한다.

그러나 실상은 다르다고 민수 형제는 고백한다. 안전가옥에서의 생활을 돌아보며 민수 형제는 '그 곳에서의 삶은 도전의 연속'이었다고 회상한다. "안전가옥에 살아가는 사람들끼리 하루가 멀다 하고 싸웠습니다. 탈북민들은 성격이 많이 거칩니다. 한 방에 대여섯 명이 같이 자는데, 어쩔 때는 말 그대로 피튀기면서 싸울 때도 있었습니다. 그렇게 싸우고 난 다음에 성경을 읽으면서 옆에 있는 형제를 마음 다해 사랑하지 못했던 것을 회개하곤 했습니다. 다들 그렇게 성품이 다듬어졌습니다."

"사실 저도 통독반 막내를 무지하게 때리고 괴롭혔던 것이 생각이 납니다. 아직도 미안한 마음이 있어요. 또 같이 살던 어떤 청년은 북한에 있을 때 태권도를 아주 잘했던 사람이라 자기 방어를 기가 막히게 했습니다. 그래서 아무도 그 사람은 함부로 못 건드렸어요." 기억을 떠올리던 민수 형제가 미소를 지으면서 말했다.

북한 사람들은 탈북을 시도하면서 수감과 고문을 포함하여 각종 충격적인 경험을 겪는다. 어쩌면 그들이 겪어야 했던

육체적, 정신적 고통이 이후 삶에서 다소 공격적인 행동으로 표출되는 것이 오히려 자연스럽다고도 느껴진다. 그 뿐만이 아니다. 그들은 탈북한 이후에도 제3 국가와 북한 당국의 비밀스러운 협작으로 인해 언제라도 신분이 발각되어 북송될지도 모른다는 끊임없는 불안과 위협 속에서 살아가고 있다.

“솔직히 제가 있던 통독반은 주님이 축복하셨던 것이 틀림이 없습니다. 3년 반 동안이나 발각되지 않은 것을 보면 말입니다. 주님께서 저희를 그동안 안전하게 보호하셨다는 고백뿐입니다.”

오픈도어 안전가옥 생활을 돌아보았을 때 민수는 그 때의 생활이 그 때 살던 모든 사람들에게 꼭 필요했던 시간이라고 회상한다. “함께 떡을 떼며 먹고 자고 하면서 자기 자신을 전부 드러내고 보여줄 수밖에 없는데, 그러면서 각자의 성품이 훈련되고 또 신앙이 성장할 수 있었던 것 같습니다. 함께 방을 썼던 다섯 명 가운데 지금은 한 명 빼고 다 목사님이 되었답니다.”

안전 가옥을 통해 역사하시는 주님

민수 형제는 자신의 경험을 비추어 볼 때 오픈도어선교회가 비밀리에 운영하는 안전가옥 사역이 탈북민들을 돌보고 그들에게 복음을 전하는 데에 있어서 대단히 중요한 역할을 하고 있다고 생각한다.

"두 가지 측면으로 나누어볼 수 있습니다. 먼저는 제가 처음 안전가옥에 들어갔을 때를 회상해보면, 그 때는 물론 하나님과 신앙에 대한 갈급함도 있었지마는 일단 머물 곳이 필요해서 들어간 것이 컸습니다. 그때의 저처럼 지금도 국경 지역에서 갈 곳이 없어 헤매고 있을 수많은 탈북민들을 생각하면 오픈도어 안전가옥처럼 그들을 따듯하게 품어주고 보호해줄 곳이 절대적으로 필요하다고 생각합니다.”

“두 번째로 중요한 이유는 지금 대한민국에 살고 있는 수백 명의 탈북민들이 알고 보면 저처럼 국경 지역 안전 가옥 출신이라는 점입니다. 저와 비슷하게 안전 가옥에서 신앙훈련을 받고서 대한민국으로 넘어와 목사가 된 북한 사람들이 꽤 있습니다. 그리고 또 목사는 아니더라도 다양한 분야에서 리더로서 준비되어 훗날 통일 이후에 북한 교회를 섬기고자 지금부터 열심으로 섬기는 동포들이 제 주변에도 많습니다.”

“그 당시에는 이렇게 될 줄 전혀 알지 못했습니다. 분명 주님께서 안전 가옥을 통해 놀랍게 역사하십니다.”

하나님이 주신 환상

민수 형제가 안전 가옥에서의 생활을 마무리할 무렵 하나님이 민수에게 어떤 환상을 보여주셨는데, 바로 북한의 교회에 대한 환상이었다. “제 몸이 붕 떠서 북한에 있던 저희 집 앞에 멈추어 섰습니다. 저희 집 앞에 포도넝쿨을 보여주셨는데, 얼마나 거대한지 장정 삼사십 명이 두 팔을 벌리고 둘러싸도 부족할 만큼 컸습니다. 그 포도넝쿨이 구름을 뚫고 올라가 한반도 전역을 뒤덮었습니다. 그 열매가 주렁주렁 매달렸는데, 어찌나 큰지 한 사람이 포도송이 하나를 겨우 들 수 있을 정도였습니다.”

“이 환상을 보면서 확신했던 것은, 하나님께서 분명히 북한의 영혼들에 대한 계획이 있으시다는 것이었습니다. 그리고 환상 가운데 저는 결단했습니다. ‘북한 선교에 저의 삶을 전부 드리겠습니다.’”

부르심의 확신을 얻은 직후, 민수 형제는 다시 북한으로 돌아가서 북한 주민들에게 복음을 전해야겠다는 마음을 먹었다고 한다. 그러나 매번 어려움에 부딪혀 돌아갈 길을 찾지 못했는데, 어느 순간 그 길이 아니라는 확신이 들었다. “북한 출신 형제, 자매님들 중에서 복음 전파에 사명을 갖고 성령님께 이끌리어 다시 본국으로 돌아가는 분들이 계십니다. 저는 그런 간증을 들을 때마다 제가 직접 갈 수 없어 죄송스러운 마음에 눈물이 앞을 가립니다.”

그러나 민수 형제는 어느 순간, 북한으로 보내시는 것 대신에 민수 형제를 대한민국 땅에서 목사로 세우셔서 훗날 북한과 남한이 하나 될 날을 준비하도록 하실 것이고, 그것이 하나님이 주신 민수 형제의 부르심이라는 것을 깨달았다고 한다.

“하나님께서는 각 사람을 위한 특별한 계획을 가지고 계신 것 같습니다. 어떤 사람들은 다시 북한으로 보내셔서 복음을 전파하도록 하시지만, 또 어떤 사람들은 남한에 머물러 남한의 삶 또한 경험하게 하시면서 훗날 통일의 시대에 남한과 북한을 이어줄 수 있는 중간다리 역할을 하도록 부르십니다. 제가 보기에 주님은 저를 후자로 부르신 것 같습니다."

라디오 사역

민수 형제는 처음 주님을 만났던 바로 그 순간을 기억하며 라디오 사역에 참여하기 시작했다. "어느 날 한 방송사로부터 연락이 왔습니다. 북한 주민들에게 복음을 전하고자 하는데 15분짜리 설교 8회 분량을 준비해줄 수 있겠냐는 요청이었습니다. 흔쾌히 수락하여 지금 작업 중에 있습니다.” 또한 그는 성경 속 다양한 주제를 다루는 라디오 방송에 게스트로 참여 중이며, 그의 목소리는 지금도 라디오 주파수를 통해 북한으로 전달되고 있다.

"라디오는 주님이 사용하시는 아주 귀한 사역의 통로입니다. 보통 될 수 있으면 더 많은 성경책이나 신앙 서적을 보내려고 하는데, 여기에는 어마어마한 방해와 어려움이 따

릅니다. 반면에 라디오 사역 같은 경우는 물건을 직접 보내거나 선교사를 직접 파송하는 것보다 위험이 적을뿐더러, 필요한 것이라곤 작디작은 라디오 기기 하나면 됩니다. 주파수와 시간대만 잘 맞추면 북한 주민들 누구든지 라디오 방송을 듣고 복음을 접할 수 있습니다. 이러한 라디오 방송 사역을 잘 활용하여 복음을 제대로 전할 수만 있다면, 북한 전역의 주민들에게 주님의 이름을 알릴 수 있는 기회가 무궁무진하다고 생각합니다."

오픈도어선교회는 라디오 방송을 통한 북한 선교 사역을 위해 한국의 다양한 방송사와 연계, 협력하여 사역 중에 있다.

민수 형제의 기도 제목

민수 형제의 가장 우선되는 기도제목은 역시 북한을 위한 기도이다. "북한 정권이 언젠가는 그 나라를 위한 진정한 통치가 무엇인지 깨닫기를 소망합니다. 정권을 지키는 것보다 먼저 북한 주민들이 굶어 죽지 않고 잘 살 수 있는 나라를 세울 수 있도록 기도 부탁드립니다."

"북한의 지하교인을 위해서 기도 부탁드립니다. 그들은 끔찍한 박해 속에서도 신앙을 잃지 않고 있습니다. 그들이 신앙의 자유를 가질 수 있도록 기도해 주십시오. 특히 성령 하나님께서 그들 가운데 강력하게 임재 하셔서 그들이 믿음을 잃지 않도록, 그리고 주님의 손이 그들을 덮으셔서 그들이 주님이 허락하신 때까지 신앙을 계속해서 지키고 살아남을 수 있도록 기도해 주십시오.

"북한의 지하 교회 교인들이 서로 협력하여 어려움을 이겨낼 수 있도록 기도해 주십시오. 여러 도움의 손길을 통해 공급되는 교육 자료와 매체들이 있는데, 그것들을 잘 활용하여 믿음의 기초를 더 견고히 할 수 있도록 기도해 주십시오. 또한 외부에서 그들의 신앙을 돕는 그 손길이 끊이지 않고 더 풍성해지도록 기도해 주십시오."

"북한은 오늘날에도 여전히 경제난에 시달리고 있습니다. 중국과 한국의 교회와 선교단체가 협력하여 북한의 지하 교회 신자들이 여러 가지 어려움을 잘 극복할 수 있도록 기도 부탁드립니다."

"혼자가 아니라는 것을 알기에 감사합니다."

민수 형제가 북한 선교라는 주님의 부르심을 향해 달려 나갈 때에 가장 큰 위로와 격려가 되는 것은 바로 세계 여러 나라의 크리스천 형제, 자매들이 동일한 기도제목으로 함께 협력하고 있다는 사실이다.

"처음 제가 신앙생활을 시작했을 때만 해도 저 혼자 살아가는 것 같아 외롭고 힘들었습니다. 그동안의 삶을 돌아보았을 때 외로운 인생길을 홀로 걸어왔어야 했고, 그랬기에 제 안에 원망이 가득했습니다."

"그러나 나중에 돌이켜 깨닫게 된 것은 저뿐만 아니라 북한의 그 어느 누구도 결코 혼자였던 적이 없다는 것입니다. 오픈도어선교회를 포함한 전 세계의 그리스도인들이 함께 이 싸움을 싸워나가고 있으며, 박해받고 고립된 신자들을 위하여 물심양면으로 기도하고 후원한다는 사실을 알았을 때 정말 큰 격려와 도전이 되었습니다. 우리 북한 사람들이 승리하며 살아갈 수 있도록 전 세계에서 이 싸움을 함께 싸워나간다는 사실이 정말 큰 격려가 됩니다."

"극심한 박해 가운데에서도 북한의 지하 교인들이 믿음을 지키고 주님의 길로 꿋꿋하게 걸어갈 수 있도록 중보해주시는 여러분들로 인해 주님께 감사드립니다. 당신들의 기도와 소망의 메시지가 북한의 지하교인들이 믿음으로 싸우고 또 승리할 수 있는 원동력이 됩니다. 저희 뒤에서 저희를 위해 기도해주시는 여러분들께 감사의 인사를 드립니다. (끝)

+ 美, 1조4000억 해킹한 北 정찰총국 소속 해커 3명 기소

〈미 법무부에 기소된 북한 정찰총국 소속 해커 3명의 모습. 이들은 세계 각국의 은행과 기업 등에서 13억달러(약 1조4000억원) 이상의 가상화폐와 현금 등을 훔치고 빼돌리려는 음모를 꾸민 혐의로 기소됐다. 왼쪽부터 미 법무부가 제공한 박진혁, 전창혁, 김일이라는 이름을 쓰는 해커들의 얼굴 사진.〉

미국 법무부가 2월 17일(현지 시각) 북한 정찰총국 소속 해커 3명을 기소했다고 밝혔다.

AP통신 등 외신에 따르면, 미 법무부는 세계 각국의 은행과 기업 등에서 13억달러(약 1조4000억원) 이상의 가상화폐와 현금 등을 훔치고 빼돌리려는 음모를 꾸민 혐의로 북한 정찰총국 소속 3명의 해커를 기소했다. 존 데머스 법무부 국가안보담당 차관보는 이들에 대해 “총이 아닌 키보드를 사용해 현금 다발 대신 가상화폐 지갑을 훔치는 북한 공작원들은 세계의 은행 강도”라고 비판했다.

지난해 12월에 제출돼 이날 공개된 공소장에 따르면 기소된 3명은 각각 박진혁, 전창혁, 김일이라는 이름을 쓰고 있다. 이들은 정찰총국 소속으로 확인됐는데, 이 기구는 ‘라자루스 그룹’ ‘APT38’ 등의 이름을 가진 해킹부대를 운용하고 있는 것으로 알려졌다.

이 3명은 악성 암호화폐 애플리케이션을 만들고 이를 통해 공격대상 컴퓨터에 백도어를 여는 방식으로 비트코인과 같은 가상화폐를 거래하는 기업들을 해킹했다. 또한 제재를 피하고 비밀리에 자금을 조달하기 위한 블록체인 플랫폼을 개발했다. 이들은 2017년 5월 랜섬웨어 바이러스인 워너크라이를 만들어 은행과 가상화폐 거래소를 해킹했고, 2018년 3월부터 적어도 지난해 9월까지 자신들이 개발한 악성 암호화폐 앱을 해커들에게 제공했다. 구체적으로 2017년 슬로베니아 가상화폐 거래소에서 7500만달러, 2018년 인도네시아 거래소에서 2500만달러, 미 뉴욕 거래소에서 1180만달러를 빼돌린 것으로 나타났다.

미 로스앤젤레스 검찰과 연방수사국(FBI)은 뉴욕의 한 은행에서 해커들이 훔쳐 2곳의 가상화폐 거래소에 보관 중인 것으로 추정되는 190만 달러어치의 가상화폐를 압수하기 위해 영장을 발부받았다고 워싱턴포스트는 전했다.

이들은 또한 미 국무부와 국방부, 미 방산업체와 에너지·항공우주 기업들에 악성코드를 심은 이메일을 보내 정보를 훔치는 ‘스피어 피싱’도 시도했다고 법무부는 전했다. 〈참고: 조선일보, 2월 17일〉

+ 김정은, 당대회 한달만에 이례적 전원회의 소집

〈김정은 노동당 총비서는 이번 전원회의에서 내각이 설정한 올해 경제목표의 문제점을 신랄하게 비판하고, 당 경제부장을 한달만에 교체했다. 연단에 선 김정은이 오른 손가락으로 한 지점을 가리키고 있는데 좌석 아래 간부를 질타하는 것으로 추정된다 (조선중앙TV)〉

북한이 노동당 제8차 대회 이후 한 달 만에 전원회의를 열고 국정운영의 문제점을 헤집고 대책을 논의해 주목된다. 당대회 이후 한 달 만에 나흘간의 전원회의를 소집한 것은 상당히 이례적이다. 이번 전원회의는 김정은 총비서가 당·내각 간부와 특수기관에 전방위로 경고를 날리며 기강을 다잡으려는 모습이다. 이번 전원회의는 애초 예정됐던 것이 아니었으나 당과 내각에서 보고한 올해 경제계획 등을 점검하는 과정에서 갑자기 결정됐을 수 있다는 관측이 나온다.

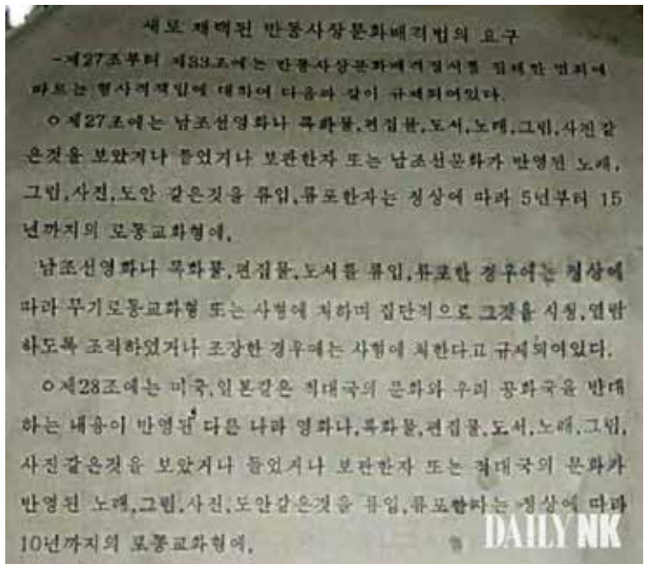
김 총비서는 전원회의 보고에서 내각에서 작성한 올해 인민경제계획의 문제점을 조목조목 지적했다. 농업부문에서 불리한 조건을 무시한 채 실행 불가능한 곡물 생산 계획을 세워 악폐를 반복했다는 점을 비판했다. 또한 전력·건설·경공업 부문에서는 비판과 처벌을 우려하며 아예 계획을 낮추는 분위기에 대해서도 꼬집었다.

특히 그는 “주요 경제부문들의 계획을 작성하는 데서 내각이 주도적인 역할을 하지 않았다”고 지적하였고, 결국 김두일 당 경제비서 겸 경제부장을 전격 해임했다. 김두일은 지난 해 말까지 평안남도 당위원장(현 책임비서) 으로 일하다가 지난달 8차 당대회에서 경제 비서로 임명됐으나 한 달 만에 좌천됐다.

인상적인 부분은 노동당을 비롯하여 국가보위성이나 사회안전성, 국방성, 군 총정치국·총참모부 등 이른바 힘센 기관인 특수 기관의 행태에 대한 비판이 거세게 이루어졌다는 점이다. 당대회에서 특수기관의 행태에 “강한 제재를 취해야 한다”고 밝힌데서 한발 더 나아가 "부문과 단체의 모자를 쓰고 자행하는 더 엄중한 반당적·반국가적·반인민적 행위"라며 “제일 장애”라고 비판했다.

북한이 당장 특수기관 산하 기업을 모두 떼어내 내각의 통제 아래 넣을 수는 없겠지 만, 이처럼 반복적으로 ‘내각중심제’를 강조 하는 만큼 적어도 큰 틀에서 특수기관들도 내각의 지휘를 받으면서 국가 경제를 우선 시하고 과도한 이익을 편취하지 못하도록 하는데 방점을 둘 것으로 전망된다. 〈참고, 연합뉴스, 2월 11-13일〉

+ 북, '반동사상문화배격법' 채택.. 남한 영상 유포자 최대 사형


새로 채택된 반동사상문화배격법의 요구

-제27조부터 제33조에는 반동사상문화배격법을 집행한 범죄에 따르는 형사책임에 대하여 다음과 같이 규제되어있다.

○제27조에는 남조선영화나 녹화물,편집물,도서,노래,그림,사진 같은것을 보았거나 들었거나 보관한자 또는 남조선문화가 반영된 노래, 그림,사진,도안 같은것을 유입,유포한자는 정상에 따라 5년부터 15년까지의 로동교화형에,

남조선영화나 녹화물,편집물,도서를 유입,유포한 경우에는 정상에 따라 무기로동교화형 또는 사형에 처하며 집단적으로 그것을 시청,열람하도록 조직하였거나 조장한 경우에는 사형에 처한다고 규제되어있다.

○제28조에는 미국,일본같은 적대국의 문화와 우리 공화국을 반대하는 내용이 반영된 다른 나라 영화나,녹화물,편집물,도서,노래,그림, 사진같은것을 보았거나 들었거나 보관한자 또는 적대국의 문화가 반영된 노래,그림,사진,도안같은것을 유입,유포한자는 정상에 따라 10년까지의 로동교화형에,

DAILY NK

〈반동사상문화배격법 설명자료에는 "많은 양의 남조선 영화나 녹화물, 편집물, 도서를 유입 및 유포할 경우 무기노동교화형 또는 사형에 처한다"고 명시돼 있다. (데일리NK)〉

북한이 남한 영상물 유포자의 최고형량을 사형으로 상향하고 반(反)사회주의 행위를 묵인한 간부의 처벌을 경고하는 등 공포 수위를 높이며 사회 통제의 고삐를 바짝 조이는 모습이다.

북한은 지난해 12월 최고인민회의 상임위 전원회의에서 '반동사상문화배격법'을 새로 채택하고 주민들이 남한을 비롯한 외부 문화에 노출되는 것을 차단하고 나섰다.

이 법은 반사회주의 사상·문화의 유입과 유포행위를 철저히 막고 모든 기관과 기업, 단체, 주민이 지켜야 할 준칙과 위반했을 경우 강력한 처벌을 담은 것으로 보인다.

세부 내용은 공개하지 않았지만, 국정원의 분석에 따르면 남측 영상물 유포자를 사형에 처하고, 시청자는 최대 징역 15년에 처하는 내용이 포함된 것으로 알려졌다.

국민의힘 하태경 의원은 2월 16일 국정원의 국회 정보위 업무보고 내용을 전하며 "쉽게 말하면 한류 처벌"이라며 "남한 영상물 유입·유포는 최대 사형, 시청은 기존 징역 5년에서 15년으로 강화했다"고 설명했다.

이 같은 통제 기류는 지난 2월 8~11일 개최한 전원회의에서도 구체적으로 나타났다.

북한은 전원회의 두 번째 의정으로 '전사회적으로 반사회주의, 비사회주의와의 투쟁을 더욱 강도 높이 벌릴 데 대해'를 상정했는데, 김 총비서는 남한 등 외부문물을 '악성종양'이라고 표현하며 "단호하게 수술해버릴 혁명적 의지와 결심"을 언급했다. 이를 위해 중앙부터 도·시·군에 이르는 연합지휘부를 조직하겠다고 밝혔다.

특히 김정은 총비서는 "반사회주의·비사회주의적 행위를 비호·조장시키는 대상을 일꾼(간부) 대열에서 단호히 제거할 것"이라고 선언했다. 이는 국가보위성과 사회안전성, 검찰기관 등 외부문물 시청을 감시 통제하는 기관과 간부들을 겨냥한 경고로 볼 수 있다.

김 총비서는 "모든 일꾼이 반사회주의, 비사회주의와의 투쟁을 저조하게 말로만 해서는 언제 가도 그것을 종식할 수 없다"며 "자기 부문, 자기 단위에서 나타나는 반사회주의, 비사회주의적 행위들을 무자비하게 억제 소멸하고 우리 식 사회주의를 공고 발전시키기 위한 투쟁에서 자기의 책임과 본분을 다해(야 한다)"고 강조했다.

김 총비서가 당 전원회의를 통해 공개적으로 단속 기관들에 경고를 한 만큼 앞으로 외부문물 시청에 대한 통제가 한층 더 강화될 것으로 예상된다. 〈참고: 연합뉴스, 2월 16일〉

+ 국제 백신 프로젝트 코백스 "북한에 코로나백신 약 200만 회분 공급"

국제 백신 프로젝트인 '코백스 퍼실리티'(COVAX Facility)는 2월 3일 잠정 백신 배분 계획 보고서를 통해 올해 상반기 중 북한에 코로나19 백신 총 199만2천 회분을 공급할 예정이라고 밝혔다. 북한에 공급될 백신은 인도 세룸인스티튜트(SII)가 생산한 아스트라제네카-옥스퍼드 백신이다.

이 제약사의 코로나19 백신은 2회 접종해야 한다는 점을 고려하면 올해 상반기 중 북한에 전달되는 백신은 99만 6천 명분에 달한다. 북한은 전체 공급분 약 199만2천 회분 중 35%~40%는 1분기, 60%~65%는 2분기에 공급받을 예정이다.

다만 보고서는 아스트라제네카-옥스퍼드 백신에 대한 세계보건기구(WHO) 측 승인과 제조사 공급 상황, 국가별 준비 상황 등에 따라 백신 공급 일정에 변동이 있을 수 있다고 설명했다.

또 해당 백신은 2월말 경 배송이 시작될 예정이지만 이 또한 상황에 따라 차후 변동될 수 있다고 보고서는 덧붙였다.

북한은 공여국들이 자금을 통해 개발도상국에 백신을 공급하는 '코백스 선구매공약매커니즘'(COVAX AMC) 대상 92개 국가 중 한

곳에 해당해 무료 혹은 저비용으로 백신을 공급 받게 됐다.

'코백스'는 코로나19 백신을 전 세계에 공평하게 분배하기 위해 세계보건기구(WHO), 세계백신면역연합(GAVI: 가비), 감염병혁신연합(CEPI) 등이 이끄는 기구이다. 코백스는 이번 보고서에서 상반기까지 145개국에 약 3억3천700만 회분의 코로나19 백신을 전달할 예정이라며, 이는 해당 국가 전체 인구의 약 3.3%에 해당한다고 밝혔다 코백스는 연내 최소 20억 회분의 코로나19 백신을 전세계에 공급하는 것을 목표로 하고 있다.

이번 백신 공급과 관련해서 세계백신면역연합(GAVI ·가비)은 "백신을 잠정적으로 배분받은 국가들은 모두 백신 신청서를 제출한 것"이라고 밝혀 북한 당국이 직접 백신을 요청한 것으로 보인다. 〈참고: 자유아시아방송, 2월 3-4일〉

북한 이해를 위해 더 읽을만한 책

제목: 북한선교의 맥(脈)
저자: 김정일, 김권능 공저
출판사: 나침반 출판사
발행일: 2020년 11월 1일
가격: 12,000원

1990년대 후반-2000년대 초반 북한선교 현장에서는 크고 작은 많은 사건들이 있었지다. 그중에서도 2001년은 6월에 있었던 최광 선교사 팀의 서안사건과 12월에 있었던 천기원 목사 구속의 굵직한 두 사건으로 기억되는해이다. 이 책의 1부를 집필한 김권능 목사는 탈북자로서 최광 선교사에게 양육을 받고 새로운 팀 개척을 위해 다른 지역으로 파송받는 등 왕성하게 활동을 하였으며 최광 선교사의 구속과 추방 이후에도 북한선교현장을 떠나지 않고 천기원 선교사를 도왔다. 당시 몽골을 통한 탈북루트를 개척하는 등 북한 선교 사역을 신실하게 이어가던 중 공안에 체포되었다. 이후로 10년간의 수감생활을 마치고 북송될 예정이었으나 하나님의 은혜로 2012년 한국으로 들어왔다. 김 목사의 사역과 수감, 출감으로부터 한국으로의 여정 스토리는 북한선교계에 널리 알려져왔는데 최근 동아일보 주성하 기자의 보도로 인해 일반 언론을 통해 소개되고 있다. 필자는 2013년 인터뷰를 위해 김권능 (당시)전도사를 만나 그의 사역이야기를 들은 경험이

있다. 당시 김권능 목사와의 인터뷰 중 그의 사역이야기를 통하여도 많은 감동을 받았지만 오히려 사역과 수감가운데 받은 많은 상처에 대해 함구하는 모습이 인상 깊었다.

이 책의 제목은 “북한선교의 맥(脈)”이다. “핵심(核心)”이라는 말은 가장 중요하고 중심이되는 부분이라는 뜻을 가진 반면, “맥(脈)” 이라하면 그 핵심들이 동질성 속에 연결된 줄기로 이해할 수 있다. “북한선교의 맥”이라는 제목에서 우리는 이 책이 북한선교의 다양한 영역의 중요한 이슈들을 다룰 것으로 추측할 수 있다.

기존 탈북민 교회-교회 내 탈북민부서와 관련되어 가장 자주 언급되는 말은“교회에서부터 이루어지는 남북통일”, “북한선교의 리트머스 시험지”와 같은 말이다. 이는 탈북민 사역에 대해 남북출신의 성도들이 잘 어우러지고 조화를 이루는, 앞으로 올 남북통일에 교회가 모델이 되어주기를 소망하는 한국교회의 시각을 드러낸다. 이런 이유로 대다수 탈북민 교회-교회 내 탈북민 부서들에 있어 남한출신과 북한출신 성도들의 비율이 하나의 평가 기준이 되기도 하며, 또한 교회의 부서구성과 사역자 구성으로부터 ‘어떻게 남한출신 성도들과 북한출신 성도들이 하나되어 성장해나갈까?’에 초점이 맞추어지게 된다.

이 책도 책의 절반을 할애하여 국내정착 탈북민 사역에 대해 다루고 있다. 그러나 이 책의 1부와 3부에서 두 저자 모두 탈북민사역과 관련하여 기존의 책들에서 다루지 않던 이야기를 하고 있다. 1부 북한 복음화를 위한 영적이해 중 “2-3. 탈북민 교회개척 필요성”에서 저자는 “굳이 탈북민들만 모이는 교회가 필요한 이유가 있을까?”라는 질문을 던지고 그에 대한 해답으로 “탈북민들이 주축이 된 교회는 탈북민들의 전도와 영적 성장에 더 효과적이다”는 결론을 낸다. 3부에서 김정일 목사는 탈북민 출신 목회자가 담임하는 탈북민 교회가 상처 입은 탈북민의 안식처로 기능할 수 있음을 실례를 들어 설명하고 있다. 이는 당연한 이야기임에도 수많은 기존도서에서는 중요하게 다루지 않던 이야기이다.

한번 생각해보자. 서구 한인사회에서 한인교회들은 낯선나라에서 지친 한인들의 안식처 역할을 감당해왔고 많은 한인들은 해외에서 만난 공동체를 통해 위로를 받고 신앙을 갖게 되었다. 해외한인교회는 “한국계”만의 공동체였으나, 오히려 이러한 한국계만의 공동체예배에서 얻는 위로와 안정감이 해외한인들의 현지적응에 큰 도움이 되었다. 돌이켜보면 기존에 쓰인 탈북민 사역 관련 책들은 대부분이 기존의 남한출신 성도들이 탈북민을 섬기거나 기존교회에서 탈북민 부서를 조직하고 사역을 활성화 하는데 초점이 맞추어진 책들이 대부분이었으며 남과 북이 조화를 이루는 모습에 초점이 맞추어졌다. 반면 탈북민에 의해 개척되어 탈북민들이 주로 모이는 교회는 실제로는 탈북민 선교의 가장 중요한 축임에도 불구하고 상대적으로 많이 다루어지지 않았다.

이 책의 1부와 3부는 중요성에 비해 많이 다루어지지 않던 탈북민 중심 교회를 강조하여 다룬 것에 의미가 있다고 생각된다. 이 책은 탈북민 교회를 다룸에 있어 남북통일의 리트머스 시험지의 역할과 같은 중대한 역할, 성도들의 남북간 출신지별 균형에 대해 언급하지 않는다. 반면 같은 경험과 아픔을 공유하고 서로의 상처를 치료하는 탈북민 신앙 공동체의 장점들을 소개한다. 저자가 말하듯 영락교회, 충현교회 같은 교회들이 본래는 실향민들로 이루어진 교회였으나 지금은 실향민교회라기보다는 한국을 대표하는 대형교회로 기억되고 있다. 우리는 이를 통해 교회가 교회의 역할을 감당하며 성장하고 시간이 흐르면 남과 북이 하나되는 목표는 자연스럽게 이루어질 수 있다는 또 다른 가능성도 생각해보게 된다.

이 책의 2부는 6명의 기독탈북민의 수기로 구성되었으며, 4부는 30년간 북한사역에 관여한 재미교포 김요셉 목사의 글로 채워졌다. 2부를 쓴 6명의 탈북민 저자 중 일부는 북한사역 관련 여러 도서에 짧게나마 소개된 적이 있는 인물들이다. 탈북민 출신으로 연세대 학부를 거쳐 미국에서 핵물리학 박사학위를 받고 대학의 연구원으로 재직 중인 죠셉한 박사의 이야기는 몇 년전 한국의 많은 언론을 통해 소개되었는데, 그의 신앙이야기는 이 책을 통해서 처음 다루어졌다. 이 책 2부 저자들의 이름을 유튜브에서 검색해보면 저자들의 더욱 구체적인 간증과 근황을 알 수 있다.

귀한 책이지만 아쉬움도 없지 않다. 먼저 책 곳곳에 역사적 사실에 대한 정확하지 않은 기록이 눈에 띈다. 가령 1부에 한경직 목사가 목회했던 도시, 북한에 있는 교회의 이름, 일제 강점기 평양 기독교인의 비율... 등의 내용에서 사소하지만 명백한 사실관계의 오류들이 발견된다. 책의 구성 또한 더 효과적으로 할 수 있지 않았을까 하는 아쉬움이 있다. 편집 과정에서 이러한 점들이 검토되고 보안되었으면 어땠을까 하는 아쉬움이 생긴다. 그럼에도 이 책은 묻어두기 아쉬운 북한선교현장의 사람들과 이야기들이 담겨 있고 탈북민사역과 관련된 주제들도 이해하기 쉽게 정리한 만큼 책의 장점을 잘 활용한다면 독자들에게 유익과 감동을 줄 것이다. 글자크기와 편집에서도 독자에 대한 배려가 묻어난다.

북한 출신 사역자들이 늘어나고, 국내 정착 탈북민 사역이 다양화되고 있다. 책을 덮으며 탈북민 사역과 관련된 도서들이 더욱 풍성하게 나눠져서 이 책과 같이 기존에 다루어지지 않던 새로운 화두가 계속해서 제기되고 다양한 결의 이야기들이 다루어지길 바래본다.

1. 최근 국제사회 여러기관에 의하여 북한의 사이버범죄에 관한 연구결과가 발표되고 있습니다. 북한의 정권차원에서 진행되는 사이버활동은 보통국가의 첩보범위를 넘어 은행, 비트코인거래소에 대한 해킹시도, 제약회사 정보 탈취시도등 민간단체와 기업에 대한 영리목적의 해킹으로 범위가 넓어졌고, 이는 국제사회에 조롱의 대상이 되고 있습니다. 최근에는 북한이 해킹을 이용해 전세계의 은행과 기업으로부터 1조 4000억원을 빼돌린 것으로 알려졌습니다. 북한정권이 더 이상 이러한 범죄행위의 주체가 되지 않도록 기도합시다.

2. 수많은 선교단체들과 기관들이 북한의 해커집단의 위협에 노출되어 있습니다. 실제로 북한의 해킹이 감지된 선교단체가 있으며, 감지되지는 않았으나 중국 혹은 북한의 해킹집단에 의해 정보가 유출된 것으로 추정되는 단체도 있습니다. 사역을 위한 커뮤니케이션으로 인해 각 단체들의 사역이 노출되지 않기를, 이를 위해 각 단체들이 적절한 보안규정과 시스템을 구축하도록 기도해주시기 바랍니다.

3. 2020년초 시작된 코로나가 현재까지 선교현장에 많은 영향을 미치고 있습니다. 북중국경의 통제가 점차 회복되어가던 중 1월말 중국과의 국경을 접한 지역에서 거리두기가 다시 강조되고 있고, 2월 초 몇몇 세관의 통제가 강화되기도 하였습니다. 선교사들중 일부는 아직도 선교현장에 들어가지 못하고 있습니다. 속히 코로나 19가 종식되고 선교현장이 문이 열릴 뿐 아니라 코로나 이후 새로운 기회가 찾아오도록 기도합시다.

4. 작년 영국에서는 코로나 극복을 위해 양로원에 마스크를 기부한 탈북민들의 이야기가 여러 신문을 통해 보도된 적이 있습니다. 그주인공 중 한명인 박지현씨가 맨체스터주 베리시 홀리루드의 구의원 선거의 보수당(현 총리 보리스 존슨이 소속된당)의 경선에 참여한다는 소식이 전해졌습니다. 한국에 정착한 탈북민들이 정치를 비롯한 사회의 각분야 주류에 진출하고 있으며 제3국 정착 탈북민들의 현지사회 정착과 새로운 도전의 소식들이 들려오고 있습니다. 각국에 정착한 탈북민들의 사회정착을 위해 기도하고 돕고있는 현지 교회들을 위해서 기도합시다.(김원호(2016), 함진우(2016), 고현철(2016)) 그리고 그 외 북에 붙잡혀 있는 조선족 사역자들의 석방을 위해서도 기도합시다. 내지 성도들을 돕기 위한 본 선교회의 사역이 국경 통제와 코로나 시국 장기화 속에서도 효과적으로 이루어질 수 있도록 기도해주십시오.

북한 기도 제목

5. 북한에 억류된 김정욱, 김국기, 최춘길 선교사와 김원호, 함진우, 고현철씨를 위해 한국교회는 지난 몇년간 열심히 기도해왔습니다. 그사이 남북관계가 급속도로 가까워진 적도 있고, 북한에 억류되있던 3명의 한국계 미국인 선교사등이 석방되는 등 희망적인 소식도 있었으나 한국인 선교사님들은 아직도 억류에서 풀려나지 못하고 있습니다. 최근 출범한 미국의 바이든 행정부가 인권을 중시하는 대외정책을 가지고 있고, 최근 캐나다를 중심으로 진행된 “자의적 구금 반대 공동 선언(Declaration Against the Use of Arbitrary Detention in State-to-State Relations)”에 주요국가들이 참여하여 목소리를 내고 있습니다(한국은 이 선언에 참여하지 않았습니다). 이러한 국제사회의 움직임이 북한에 압력을 가하고 이것이 한국 선교사님들의 석방으로 이어지도록 기도합시다.

6. 라디오는 복음을 북녘을 향해 전달하는 효과적인 수단입니다. 오픈도어선교회는 생명의 강 방송, 극동방송, 북방선교방송과의 협력을 통해 북한의 성도들을 격려하고 주민들에게 복음을 전하고자 애쓰고 있습니다. 2021년 새로운 프로그램을 가지고 북한으로 복음의 메시지를 송출할 이들 방송국들과 방송사역자들을 위해 기도합시다. 북한의 성도들과 주민을 위한 양질의 방송이 제작될 뿐 아니라 들으시는 청취자들이 안전한 가운데 복음의 메시지를 온전히 듣고 깨닫는 역사가 충만하도록 기도합시다. 기상 악화나 북한의 방해전파 등으로 인한 음질 저하 및 청취 장애가 발생하지 않도록 기도합시다.

서울시 동작 우체국 사서함 56호 우편번호 07056
* TEL 02-596-3171
* Home Page : www.opendoors.or.kr
* E-mail : info@opendoors.or.kr

▣ 후원계좌 (북한선교)
국민은행 (한국오픈도어선교회)
029301-04-169183

북한월간개발소식 / 등록일 : 2010년 9월 27일 / 등록번호 : 성북, 라 00067 / 발행년월일 : 2021년 3월 1일

Open Doors

World Watch List 2021 월드와치리스트 - 기독교박해지도

크리스천들을 가장 박해하는 국가 TOP 50

1 북한
2 아프가니스탄
3 소말리아
4 리비아
5 파키스탄
6 에리트레아
7 예멘
8 이란
9 나이지리아
10 인도
11 이라크
12 시리아
13 수단
14 사우디아라비아
15 몰디브
16 이집트
17 중국
18 미얀마
19 베트남
20 모리타니아
21 우즈베키스탄
22 라오스
23 투르크메니스탄
24 알제리
25 터키
26 튀니지
27 모로코
28 말리
29 카타르
30 콜롬비아
31 방글라데시
32 부르키나파소
33 타지키스탄
34 네팔
35 중앙아프리카공화국
36 에티오피아
37 멕시코
38 요르단
39 부르나이
40 콩고
41 카자흐스탄
42 카메룬
43 부탄
44 오만
45 모잠비크
46 말레이시아
47 인도네시아
48 쿠웨이트
49 케냐
50 코모로

박해수준

극심한 수준의 박해 매우 높은 수준의 박해

오픈도어 월드와치리스트는 크리스챤의 박해가 가장 심한 50개 국가들의 순위를 정한, 독보적이고, 종합적이며, 신뢰할수 있는 자료입니다. 오픈도어 분석가들이 150개 국가의 현장으로 부터 오는 실제적인 데이타를 분석하여 만들어진 것입니다. 각 국가의 박해수준은 오픈도어가 이용하는 평가 점수 시스템에 의해 기록됩니다. 이것은 폭력만을 고려하는 것이 아니라 크리스챤들이 개인과 가정과 교회와 사회 생활 가운데 얼마나 자유롭게 신앙생활을 할 자유가 보장되는지를 평가하는 것입니다.

오픈도어의 조사 방법과 결과물은 국제종교자유기구 (International Institute for Religious Freedom)에 의해 감사를 받습니다. WWL2021 데이타는 2019년 10월1일부터 2020년 9월30일까지 기간에 해당됩니다.

"내 삶과 조국을 위해 내 마음과 꿈을 다시 여는 데는 오랜 시간이 걸렸습니다. 그 과정은 민주주의 사회에 정착한지 몇 년이나 지난 후, 더 중요하게는 많은 기도를 통해 그리고 하나님의 사랑을 받아들이는 것을 통해 이루어졌습니다. 하나님의 사랑은 얼어붙은 나의 마음을 녹였습니다. 오늘 열린 마음으로, 나는 북한에 대한 나의 꿈과 희망의 아름다움을 보고 있습니다" 탈북 디모데 형제

"너희도 함께 갇힌 것 같이 갇힌 자를 생각하고 너희도 몸을 가졌은즉 학대 받는 자를 생각하라"

히13:3

한국 오픈도어 선교회

www.opendoors.or.kr