My home backup and minimal security system

I've recently experienced what is it like to have an "uninvited guest" in your home while you're away hiking - hint: it doesn't feel good. Since then I decided to finally put together the things I've been postponing for months for various reasons - mostly for being lazy.

The need for some security, or at least the illusion of it

The reasons are not much to stop burglars from coming in but to have both some proof in case something happens and to assure I've done everything in my power to prevent it. Locks and doors here, in the UK, are jokes compared to Eastern Europe, but unlike Eastern Europe, the insurance companies actually pay out, so instead of trying to physically secure our place I'm trying to prepare for proving if something happened. They were nice and immediate with out first ever claim, but I'm not certain they would be with a second one if I have no proof. Also because our landlord doesn't allow us to make any alterations, so physical security is what is provided.

0. Register your items

This was the one of the biggest mistakes I ever made: not registering as much identification of our items as possible. For the UK, there is a site, called immobilise[^1], which is used by the police as well, and even if you're not in the UK, it may be very useful as an inventory list. Do add MAC addresses besides the serial numbers; the serials, unfortunately, can be removed from most products too easily.

1. Camera: Raspberry Pi + Pi NoIR[^2] + motionEyeOS[^3]

A security camera does not give you physical security. It is to secure your statement in case the police or an insurance company questions your word. It's also a good tool to check upon your property, for example, after a big storm if you're away, or check on your pets.

The Raspberry Pi is cheap and is an extremely flexible tool to have. There is an official camera modul and an official, no infrared filter camera module - this latter is of course for night vision.

While I'd love the system to have a full-blown Debian on it, I've found installing Motion[^4] on Raspbian problematic and unstable - therefore I ended up flashing motionEyeOS on a microsd. Much less flexible, much more robust and reliable.

It has a ~~little too fancy web~~ interface, with an included web view of the stream. It comes with numerous features out of the box, such as automated uploads to Google Drive, which I found extremely useful. Yes, you could hack a system like this together on your own, but this is a good system, and it's stable.

Why not an off the shelf solution?

I've tried one of the medium range Foscam cameras - ended up sending it back within an hour. The main reason was that the video stream was only available through a browser addon and only for Windows and Mac. It was also very limited on features, especially for fine tuning.

It was, however, pretty stable, so if this is OK for you, go for it; hacking is only required when you can't find anything good enough for you needs.

2. Alarm system

I've bought a Yale HSA6400[^5]. This is a pre-packaged set of:

- a head unit with phone line capabilities (requires a landline, can call 3 numbers on alert and can be remotely armed and disarmed, but it's really, really old school)
- a fake
- and a real siren
- 2 infrared motion sensors
- 2 door contacts

This is usually enough for a regular flat or a small house, although I had to add some keyfobs as well.

Why an off the shelf solution?

Because putting together an alarm system is not as easy as it sounds and is definitely more expensive you first think it will be. All units have built-in tamper switches - they are usually plain spring switches, but they are there -, all of them have backup batteries, including the siren and the main unit, and they last ~2 years from their battery. Replicating all of these is not easy.

Improvements and possible future transition

I bought the HSA family for two reasons:

1. it's cheaper than the new ones
2. is uses 433 MHz

The 433MHz is the most common frequency family that is used in this area and I hope to be able to sniff any status changes with an Arduino later on; maybe even transition to a self-made solution once.

I've found a mad hacker who added GSM and other capabilities to a similar system, but I'm nowhere near to his skills. It's an interesting video anyway and there are lots of things to learn from it: Yale HSA6400 Burglar Alarm Arduino modifications - Part 1[^6]

3. Home + remote backup server

This is for a different security: for your digital life. While both me and my wife are having less and less real life valuables - there are things valuable to us, memories mostly, but those doesn't worth money - the number of our digital valuables are growing and they need safe storage places.

For this reason I ended up using an my old ThinkPad T400[^7] as a home server. You can add 2 disks in there, which could give you a 2x2TB software RAID 1 or a 4TB software RAID 0 at max. It has battery back up, a SIM card and a modem built in, and it's probably the most quiet laptop they ever made, so perfect for a non-CPU intensive home server.

Apart from this, I have a rented server from Hetzner[^8]. This German company does something very unusual: they have a server bidding[^9], where they reuse older models and give them for a very reasonable price. Mine is a 2x3TB i7 2600 machine with 16GB RAM - for 29.90EUR/m. They also offer cheaper "Storage Boxes", but those doesn't seem to have rsync and an option.

Why not just remote?

I keep the home server for various reasons. The main one if that I need a buffer. My internet upload speed caps out at ~1200Kbps, which means uploading GBs of pictures takes a long time. This we can't always afford to wait out sitting at our laptops, not having a copy of the valuable memories. The local server makes the initial copy fast, so we can take the laptops away from the home internet connection.

It is also another copy. The Hetzner machine serves some websites and it's an internet facing beast, which means it's under a constant threat of someone finding a way to hack it, deleting all the backups there.

It has a built-in SIM slot with a modem so I can use it as an SMS server. This is good when the local network is up, but the internet is down; it can notify me if the system is still fine. The afromentioned Raspberry Pi can also use it to send motion detection notifications - even when there is no internet connection, so mail or webhooks are not an option. I know many hate SMS messages, but they are still the most convenient way to reach someone fast.

Encrypted backup partitions

Having my "valuable" data on a rented server where the disk is not mine gives me a bit of paranoia, therefore encryption was required there. It's not the same with the local server, though I ended up encrypting the backup partition there as well. I've read stories of data dug up from used hard drives and I do not want that happen to me.

This obviously make data recovery hard - let's say near impossible - in case the machine dies, but since there ~~are~~ should be 3 copies of the data at least, the need to recover a disk is very unlikely.

I've been bitten by encryption recently, but that was because the install process of FreeBSD forgets to tell you that using full-disk encrypted ZFS is dangerous. Actually, using full-disk encrypted system is always dangerous and probably suicide on a server, because on an unexpected power loss it won't reboot. *Or, as with FreeBSD, it will corrupt the filesystem, let you sweat for hours before you give up and reinstall a Debian.* That is not what you want from a server.

Therefore what I ended with is the following:

- software (md) RAID 1 for a small root partition; ext 4, not encrypted
- software (md) RAID 1 for a swap partition
- software (md) RAID 0 for the backup partition, LUKS encrypted, btrfs on top

RAID 0 because I have 2x1TB disk and otherwise the space is not enough. LUKS on top of the md device, so the data is encrypted. btrfs because zfs-on-luks sounds horrible and the zfs for linux doesn't have encryption yet, and because I wanted on-the-fly, transparent compression on the filesystem. So it was either NTFS - which is a brilliant fs, but not for linux - or btrfs.

Don't do btrfs if your kernel is < 3.18.

This is how it's done

```bash
#!/bin/bash

apt-get install cryptsetup-bin
# choose the device carefully, this is my own case
DEVICE="/dev/md2"
BACKUP="backup"
cryptsetup -v --cipher aes-xts-plain64 --key-size 256 --hash
sha256 --iter-time 2000 --use-urandom --verify-passphrase
luksFormat "${device}"
cryptsetup luksOpen "${device}" "${BACKUP}"
```

```
mkfs.btrfs "/dev/mapper/${BACKUP}"
mkdir -p "/${BACKUP}"
mount -o noatime,autodefrag,compress=lzo,noacl "/dev/mapper/$
{BACKUP}" "/${BACKUP}"
```

btrfs has a useful feature, called scrub. This checks data integrity and can save you from data rot[^10]. Running `btrfs scrub start` regularly helps - in theory.

4. Archives

With the sad rise of ransomware[^11] and the less known possible corruption of filesystems, mutable copies of files - backups - are not safe enough copies.

I've made some digging on what to use as long-term, archival, cheap storage and I ended up with two solutions a regular person can afford:

- Blu-Rays
- Amazon Glacier

I prefer the first.

Blu-Ray seems to be designed in a very different was CDs and DVDs were, mostly to last longer. Panasonic claimed for a long time, that their ordinary, single layer, 25GB Blu-Rays can last for 50 years, but they recently removed this logo from their packages, introducing the more expensive, archival grade ones. I still think the regular disks are viable options for 10-20 years, which is puts them in the league of tape drives.

There is also the option of M-Disc[^12], "clinically" proven to last for 1000 years; unfortunately they are a bit too expensive for my taste and it's arguable if it really does have that many benefits over plain Blu-Ray.

Anything that you think irreplaceable you should put it on something that cannot easily be deleted.

5. Summary

Home security is not only about physically securing your place. While a physical security - massive metal door, thick, brick walls, etc - are of course good to keep people out, they are unfortunately good to keep you in or out as well, if you lose you keys or when you need to escape.

If you happen to be in a country where insurance is a thing, has a long history, and insurance companies do pay out, get one as soon as possible, and do revisit your contents policy from time to time.

Electronics themselves are replaceable; all of them. It is necessary to register them or have an inventory list, including serial numbers, MAC addresses, and unique markings; sometimes even photographs, it there are markings which cannot be hidden if someone is about to sell the item.

The valuable part of electronics are their data. If something is stolen or lost, take precautions: change password as soon as possible, force logouts from services. Use encryption, but be careful with that, as it may be a pain in the ass.

Have backups, preferably more than one. Do not rely on a single backup and test if your backup contains all the data you think it does.

Make regular archives. Blu-rays are not that cheap, but losing memories cost more.

Links

1. https://www.immobilise.com/
2. https://www.raspberrypi.org/products/pi-noir-camera/
3. https://github.com/ccrisan/motioneyeos
4. http://www.lavrsen.dk/foswiki/bin/view/Motion/WebHome
5. http://www.yale.co.uk/en/yale/couk/ProductsDB/?groupId=4326&productId=59213
6. https://www.youtube.com/watch?v=TvWwp9kR7dU
7. http://www.thinkwiki.org/wiki/Category:T400
8. https://www.hetzner.de/gb/hosting/
9. https://robot.your-server.de/order/market/country/GB
10. https://en.wikipedia.org/wiki/Data_degradation
11. https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise
12. http://www.mdisc.com/